UNIVERSIDAD DE COSTA RICA

Control Interno

BOLETÍN TÉCNICO **2025**

ISSN: 2215-4485

Contraloría Universitaria
UCR

Índice

Presentación

MBA GLENN SITTENFELD JOHANNING

Estimados lectores del Boletín Técnico de Gestión y Control 2025, es un honor presentar un nuevo ejemplar que refleja el compromiso de la Oficina de Contraloría Universitaria con la promoción de buenas prácticas, el fortalecimiento del control interno y la generación de valor público para la comunidad universitaria. En un contexto nacional que avanza hacia la implementación de los nuevos Estándares Globales de Auditoría Interna (NOGAI), resulta indispensable continuar desarrollando nuestras competencias, adaptarnos a los cambios normativos y aprovechar las oportunidades que ofrecen la tecnología, la gestión del conocimiento y la gobernanza de datos para las auditorías internas del sector público.

Este boletín reúne una serie de artículos elaborados por compañeras y compañeros de la Oficina, quienes comparten sus experiencias y reflexiones sobre temas de gran relevancia para nuestra labor. Iniciamos con “Competencias, un componente fundamental para los equipos de auditores”, donde se resalta la importancia del desarrollo profesional continuo, alineado con el Dominio II de los NOGAI. Seguidamente, el artículo “El salario global en la Universidad de Costa Rica” ofrece una visión clara del régimen salarial y los retos que representa para la gestión institucional. En “Seguridad de la Información” se analizan los principios esenciales para proteger los activos de información, cada vez más expuestos a riesgos y ciberamenazas. Por su parte, “Estudio del cumplimiento del régimen de dedicación exclusiva” presenta experiencias aprendidas en la fiscalización de esta figura contractual. Asimismo, “Importancia de la gobernanza de datos institucionales en los procesos de auditoría interna” muestra cómo el uso estratégico de los datos fortalece la toma de decisiones y la eficacia del control. Finalmente, el artículo “Evaluación del riesgo de control interno” destaca la necesidad de anticiparnos y gestionar los riesgos como elemento central del sistema de control interno.

Espero que estos aportes sean de utilidad en el ejercicio de sus funciones y contribuyan a la mejora continua de nuestra gestión en el quehacer institucional. Agradezco sinceramente a todas las personas que colaboraron en la elaboración de este boletín, así como a quienes día a día fortalecen el sistema de control interno institucional con su compromiso, ética y dedicación. Les invito a seguir innovando, aprendiendo y construyendo juntos una universidad más eficiente y transparente orientada al cumplimiento de las políticas y el plan estratégico en aras de seguir generando valor en la ejecución de sus actividades sustantivas.

OCU
BOLETÍN

Competencias, un componente fundamental para los equipos de auditores

LICDA. MARIELA PÉREZ IBARRA, CPA
Subcontralora Universidad de Costa Rica

mariela.perez@ucr.ac.cr

En un partido de futbol el equipo ganador es quien logra anotar más goles, en un partido de baloncesto ganan si encestas más canastas que el equipo contrincante, en voleibol ganan los que logran que la bola no rebote dentro de su espacio de juego. En todos estos ejemplos, cada una de las personas que participan tienen claridad de que tiene que hacer, cómo lo pueden hacer y practican los movimientos que les permite ejecutar la acción requerida de forma efectiva y eficiente. Deben ser competentes para ganar el juego, ese es su objetivo.

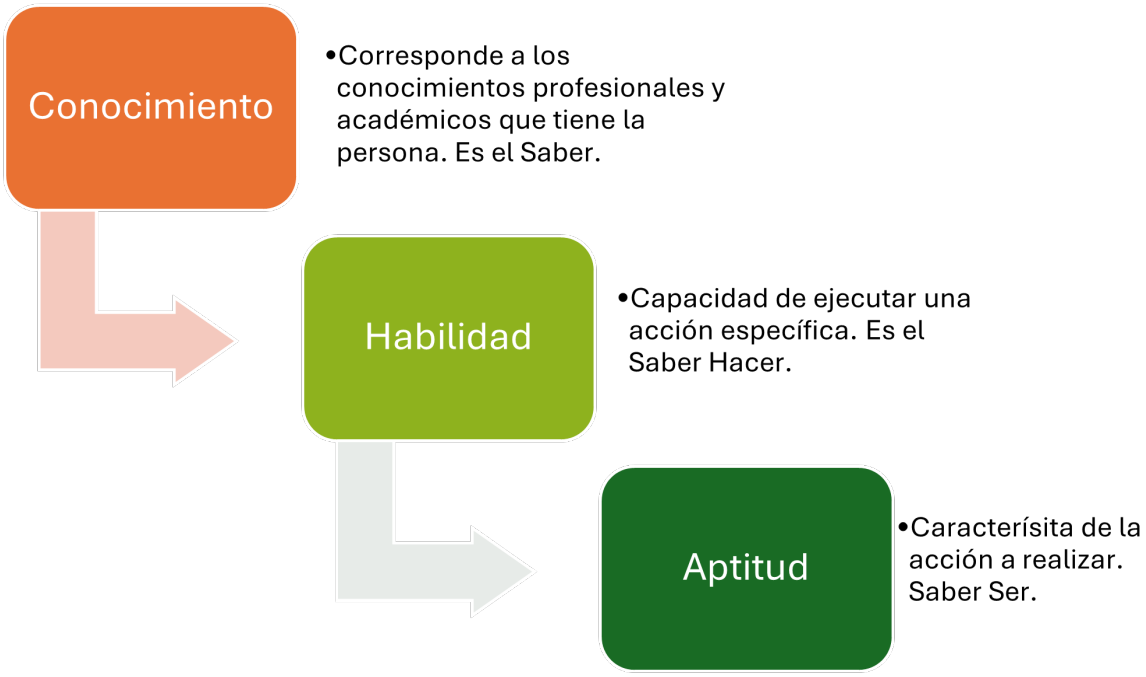
Al igual que en los equipos deportivos, en las organizaciones las personas son el medio para lograr los objetivos propuestos, y para ello es fundamental reconocer en el equipo de trabajo las capacidades de sus integrantes. En este sentido, la institución tendrá un porcentaje mayor de probabilidad de éxito si es consciente de quienes son los colaboradores y cómo influyen en los procesos internos. Por tanto, la gestión por competencias es útil para determinar características de un colaborador en relación con el coaching, mentoría, liderazgo, pensamiento crítico, ética, comunicación efectiva, escucha asertiva, entre otros. Con esta información quien toma decisiones, al igual que lo hacen los directores técnicos de los equipos deportivos, lograran visualizar quienes son las personas más competentes para cada cubrir un puesto y ejecutar una acción determinada.

Para las auditorías internas las Normas Globales de Auditoría Interna (NOGAI), específicamente en el Dominio II. Ética y Profesionalismo, presentan en el principio 3. Demostración de Competencia, elementos necesarios para una adecuada gestión por competencias del auditor interno y su desarrollo profesional continuo.

Este principio indica que una competencia se define como:

Figura N°1

Componentes de las Competencias



La determinación de conocimientos, habilidades y aptitudes permite determinar aspectos que influyen en los resultados en la ejecución de las actividades realizadas. Con esta información se gestiona de manera adecuada las brechas determinadas entre lo esperado y lo logrado; así mismo, se definen los comportamientos esperados de los auditores al momento de realizar sus funciones.

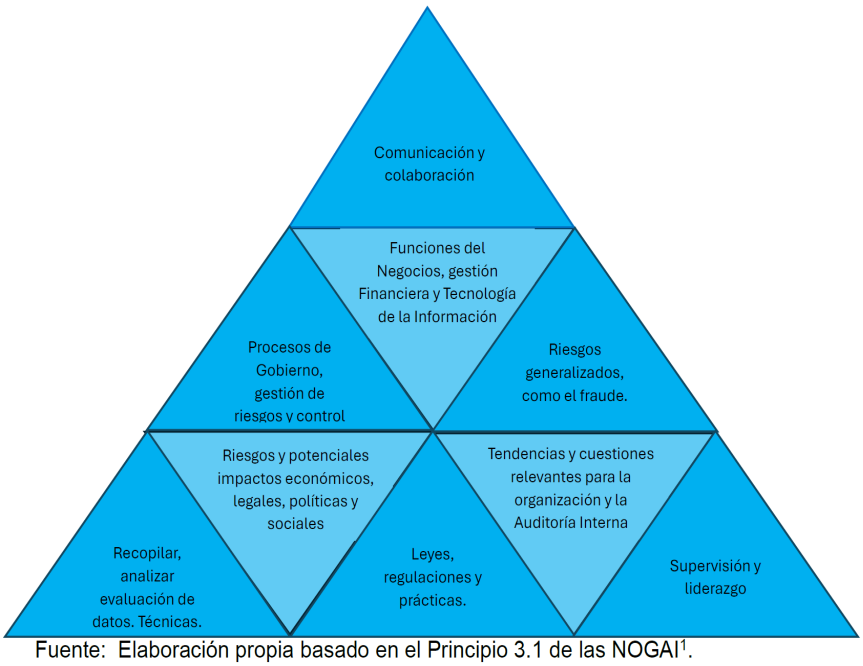
Estos elementos fundamentan apropiadamente la toma de decisiones para cumplir con los objetivos, desde:

- La definición de los puestos del departamento de auditoría.
- Las responsabilidades correspondientes a las actividades a ejecutar.
- Los conocimientos requeridos para llevar a cabo estas actividades de forma apropiada.
- La definición apropiada de los elementos requeridos para la evaluación del desempeño.
- La información necesaria a considerar el cuadro de remplazo que se requiere para dar continuidad a los procesos.

Además, este Principio 3. incorpora la Norma 3.1 Competencia, en la cual se enumeran en el apartado de "Consideraciones para la implementación", 9 temas en que se debe desarrollar las competencias del auditor interno, a saber:

Figura N°2

Competencias de los auditores internos.



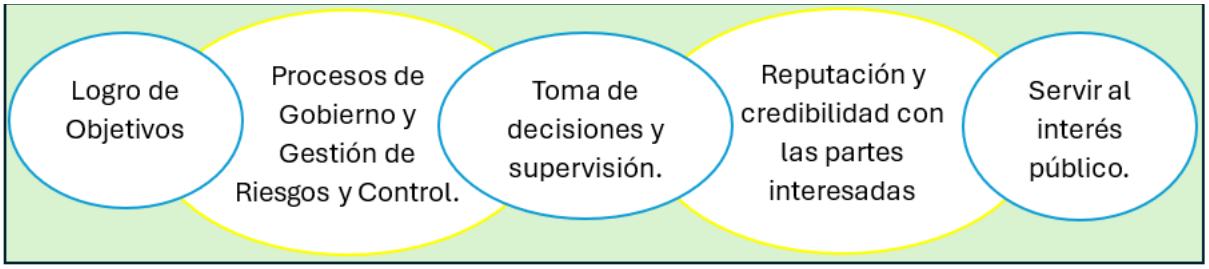
Fuente: Elaboración propia basado en el Principio 3.1 de las NOGAI[1].

[1] Tomado de las Normas Globales de Auditoría interna 2024, The Institute of Internal Auditors.

Las competencias mencionadas en esta normativa permiten la actualización de los procedimientos de la auditoría interna basados en las necesidades actuales de la organización en la cual están inmersa mediante la contribución en el logro de sus objetivos estratégicos, tal y como se presenta en la siguiente figura:

Figura N°3

Áreas en que la auditoría interna contribuye en la organización



Fuente: Elaboración propia basado en el Dominio 1 de las NOGAI [1]

El contar con un Manual de Puestos que describa las actividades específicas a realizar del personal del equipo de auditoría, sus responsabilidades, requisitos y competencias, permite al Director de Auditoría Interna tener la información completa y actualizada que se requiere para cumplir con lo indicado en la Norma 3.1, específicamente en:

- Mantener información sobre las competencias de los auditores internos para utilizar en la asignación de tareas, la identificación de las necesidades de formación (capacitación) y en el reclutamiento de auditores internos para cubrir los puestos vacantes.
- Participar en la revisión del desempeño de cada auditor interno.
- Identificar las áreas en las que las competencias de la Función de Auditoría Interna deberían mejorar.
- Animar a la curiosidad intelectual de los auditores internos e invertir en la formación / Capacitación y en otras oportunidades para mejorar el desempleo de Auditoría Interna.
- Comprender las competencias de los otros proveedores de servicios de aseguramientos y asesoramiento, y considerar la posibilidad de confiar en ellos como fuente de competencias adicionales o especializadas que no se encuentran disponibles dentro de la Función de Auditoría Interna.

[1] ídem 1.

- Considerar la contratación de un proveedor externos de servicios cuando la Función de Auditoría Interna, colectivamente, no posee las competencias necesarias para proporcionar los servicios solicitados.
- Implementar el Programa de Aseguramiento y Mejora de la Calidad de forma eficaz. [1]

Para el diseño de puestos, lo esencial es realizar una descripción clara de las actividades, funciones y responsabilidades que ejecutarán cada una de las personas que realizan los servicios de auditoría interna definidos en el Glosario de la NOGAI, como:

> **Auditoría Interna** – Una actividad independiente y objetiva de aseguramiento y asesoramiento diseñada para añadir valor a las operaciones de una organización. Ayuda a la organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gobierno, gestión, de riesgos y control. [2] (El subrayado no es del original.)
>
> **Servicios de aseguramiento** – Servicios a través de los cuales los auditores internos realizan evaluaciones objetivas para proporcionar aseguramiento. Entre los ejemplos de servicios de aseguramiento se encuentran los trabajos de cumplimiento, financieros, de la operativa, de desempeño y de tecnología. Los auditores internos podrán proporcionar aseguramiento limitado o razonable, dependiendo de la naturaleza, el momento o la extensión de los procedimientos ejecutados.
>
> **Servicios de asesoramiento** – Servicios a través de los cuales se ofrece asesoramiento a las partes interesadas de la organización sin proporcionar aseguramiento ni asumir responsabilidades de gestión. La naturaleza y alcance de los servicios de asesoramiento están sujetos al acuerdo efectuado con las partes interesadas relevantes. Los ejemplos de estos servicios incluyen el diseño e implementación de nuevas políticas, procesos, sistemas, y productos; servicios forenses; formación (capacitación); y la facilitación de debates sobre riesgos y controles. Los "servicios de asesoramiento" también se conocen como "servicios de consultoría". [3]

---

1 Ídem 2.
2 Ídem 2.
3 Ídem 2.

Estos conceptos son el punto de partida para definir las tareas de los colaboradores del equipo auditor, ya que se logra definir que competencias son necesarias para cumplir con los servicios a brindar considerando conocimientos, habilidades y aptitudes[4] requeridas. Alineado a las NOGAI, el IIA también publicó el Marco de Competencias de Auditoría Interna, en el cual desarrolla las competencias y conocimientos en las siguientes categorías:

- Competencias de auditoría interna
- Competencias profesionales
- Competencias de gobierno y gestión de riesgos
- Competencias del área operativa

Además, establece la necesidad de considerar en qué nivel se ha desarrollado en cada persona la competencia respectiva y para ello establece estos niveles en básica, intermedia, avanzada y experta.

El cómo convergen los tres elementos de una competencia lo explica el Dr. Mario Alonso Puig, neurólogo de gran trayectoria, en su libro Tus Tres Super Poderes que expone lo siguiente:

> No hay manera de convertir un conocimiento en habilidad, no se puede convertir el saber en saber hacer si uno no pasa a la acción de una forma consistente. Si queremos que los nuevos conocimientos y descubrimientos que hagamos se conviertan en una forma nueva y mejor de ser y de estar en este mundo, tenemos que integrar lo aprendido en la musculatura, esto es, en el inconsciente, y esto solo se logra a través de un determinado entrenamiento y de una disciplina sostenida.

La intencionalidad de ser consciente de lo que se quiere aprender y hacer bien es parte de la actitud y aptitud de la persona, que en consecuencia es lo que refuerza la conducta de la persona y refleja su nivel de competencia. En concordancia con lo anterior, es lógico entender por qué la demostración del cumplimiento de las competencias se determina en conductas observables; por ello la conducta se define y evalúa en una escala conductual, logrando identificar quienes dominan totalmente una competencia hasta quienes podría cumplirla parcialmente. Es en este reconocimiento que existe la posibilidad de que se pueda ir mejorando el nivel de ejecución de una tarea mediante la realimentación de los resultados obtenidos en la evaluación del desempeño.

4 Definición de competencia de acuerdo con el apartado de Glosario de las NOGAI.

En conclusión, las auditorías internas y sus equipos de trabajo tienen una gran oportunidad de mejorar su gestión considerando las competencias requeridas de acuerdo o lo indicado por las NOGAI, lo cual permitirá tener con claridad las actividades a ejecutar en cada una de las plazas asignadas, sus responsabilidades y su contribución en la consecución de los objetivos estratégicos. Así mismo, podrá determinar brechas en los comportamientos ejecutados por sus colaboradores, mediante las evaluaciones del desempeño con lo cual se podrá determinar si la persona auditora requiere de actualización de conocimientos, mejora en las habilidades o en la aptitud para ejecutarla. Él éxito de un equipo deportivo se basa en que el entrenador conoce a los miembros de su equipo y logra que todos conozcan con claridad como ganar el juego, que deben hacer para ganarlo y como aplicar ese conocimiento en sus acciones. En las auditorías internas el éxito se comprobará cuando la gestión de los equipos de auditores muestra a sus usuarios los resultados de las actividades ejecutadas y estos resultados impacten de forma positiva en el logro de los objetivos propuestos por la organización.

OCU
BOLETÍN

El Salario Global en la Universidad de Costa Rica

MBA. MADELAINE CARMONA P.
Auditora

madelaine.carmonaprado@ucr.ac.cr

La Constitución Política de Costa Rica, regula en sus artículos 191 y 192 las relaciones entre el Estado y los servidores públicos, esta relación de empleo es de carácter estatutario y su propósito es garantizar la eficiencia de la administración.

El 09 de marzo de 2022, después de varios intentos en las últimas décadas con varios proyectos, se publica la ley 10159 "Ley Marco de Empleo Público", en Diario Oficial La Gaceta (Alcance N°50 a la Gaceta N°46), la cual rige doce meses después de su publicación. Esta ley, contiene una serie de regulaciones atinentes a las relaciones de empleo de los funcionarios públicos (reclutamiento y selección, evaluación del desempeño, permisos, remuneraciones, entre otros).

El ámbito de aplicación de esta ley se estableció en el artículo 2:

ARTÍCULO 2- Ámbito de cobertura

Esta ley es aplicable a las personas servidoras públicas de las siguientes entidades y órganos bajo el principio de Estado como patrono único:

a) Los Poderes de la República (Ejecutivo, Legislativo y Judicial), sus órganos auxiliares y adscritos, y el Tribunal Supremo de Elecciones (TSE), sin perjuicio del principio de separación de Poderes establecido en la Constitución Política.

b) El sector público descentralizado institucional conformado por: las instituciones autónomas y sus órganos adscritos, incluyendo universidades estatales, la Caja Costarricense de Seguro Social (CCSS), instituciones semiautónomas y sus órganos adscritos, y las empresas públicas estatales.

c) El sector público descentralizado territorial conformado por las municipalidades, las ligas de municipalidades, los concejos municipales de distrito y sus empresas.

(Subrayado no es del original)

Expresamente se incluye a las universidades estatales, de la cual la Universidad de Costa Rica forma parte, en el ámbito de aplicación de la ley, la cual comprende un conjunto de normas que regulan las relaciones estatutarias entre la Administración Pública y los servidores públicos con el objetivo de establecer un único régimen de empleo público.

Antecedentes

El sistema salarial de la Universidad de Costa Rica es el resultado de una mezcla de incorporaciones e interpretaciones técnico-jurídicas, tanto internas como externas, que a través de los años han dado como resultado un sistema salarial híbrido y altamente complejo en su administración y gestión institucional.

Desde el año 2014 la Institución ha venido tomando medidas para la contención del gasto de salarios y a partir de la aprobación de la Ley 9635 "Ley de Fortalecimiento de las Finanzas Públicas", la cual empezó a regir el 04 de diciembre de 2018, fecha de su publicación en La Gaceta, misma que para el título III y decreto ejecutivo N° 41564- MIDEPLAN-H que lleva por título "Reglamento del título III de la Ley de Fortalecimiento de las Finanzas Públicas, Ley N°9635 del 3 de diciembre de 2018, referente a empleo público", las universidades públicas presentaron en el año 2020 un recurso de inconstitucionalidad por incorporar de manera indebida a las instituciones de educación superior estatal.

A pesar de estar en espera de una respuesta por parte de los tribunales sobre la aplicación de dicha Ley, la Universidad se ha visto obligada a adoptar, de manera precautoria, varias medidas a efecto de ajustar el sistema salarial de la UCR en temas de:

- Anualidad
- Cesantía
- Dedicación exclusiva
- Prohibición
- Nominalización de incentivos salariales
- Topes y aumento salariales

Con el fin de mitigar el riesgo en caso de que las resoluciones posteriores de los juzgados impliquen erogaciones mayores para la Institución. Asimismo, la pandemia generada por el COVID-19 en el año 2020, y el debilitamiento de las finanzas mundiales, obligó a adoptar nuevas medidas para ajustarnos al presupuesto aprobado por la República.

El Sistema Salarial es un tema de vital importancia para la Universidad porque el mismo representa el rubro presupuestario más alto dentro de la estructura de costos de la institución.

La planilla institucional experimenta cambios relevantes, hecho que demanda necesariamente que los ingresos crezcan en la misma proporción, con el propósito de evitar un desequilibrio financiero, además, en los últimos años, ha sido fuertemente cuestionada por el poder ejecutivo y otros órganos del gobierno quienes señalan que la UCR posee algunos conceptos de pago bastante altos.

El sistema salarial universitario

Anterior a la entrada en vigor de la Ley 10159, la Universidad de Costa Rica ha mantenido un salario compuesto, el cual es definido como: Salario base más componentes salariales complementarios (sobresueldos, pluses o incentivos).

La Universidad de Costa Rica cuenta con una población laboral promedio de 9639 funcionarios, los cuales realizan tanto labores docentes como administrativas. Para cada sector, tanto el docente como el administrativo existen diferencias en su estructura salarial, ya que cada uno se regula con su propia normativa.

- Sector docente de la Universidad de Costa Rica

El Régimen Académico de la Universidad de Costa Rica es el sistema que organiza a los profesores universitarios en categorías con base en sus méritos académicos y en su experiencia universitaria, dichas categorías se encuentran establecidas en el Reglamento de Régimen Académico y Servicio Docente de la Universidad de Costa Rica (Aprobado en la Sesión 2869-17 del 16/02/1982, publicado en La Gaceta Universitaria 76-82 del 22/04/1982. Modificación parcial aprobada en sesión 5297-11 del 4/10/2008, publicada en La Gaceta Universitaria 41-2008, 24/11/2008).

El régimen salarial académico es el sistema que regula las remuneraciones salariales del personal académico universitario y los puestos de dirección. Cubre sin excepción a todas las personas contratadas por la Universidad de Costa Rica para realizar tareas académicas, de investigación y acción social.

Hasta principios del año 2024, con la implementación del Reglamento de Régimen Salarial Académico el cual discutiremos más adelante, el salario de las diferentes categorías docentes se conforma adicionando al salario base de la categoría más baja, un porcentaje que varía según diferentes aspectos que considera el régimen de méritos del sector, tales como, títulos obtenidos, publicaciones realizadas, evaluaciones en el área docente, investigativa o de acción social, puntaje que define en cual categoría se ubica un docente en régimen y así su respectiva remuneración base, adicionando los diferentes conceptos de pago propios de esa persona.

Ejemplo del Salario Compuesto de un docente de la UCR

Detalle de Salario: Profesor Catedrático "AAR"		
Salario Referencia	Escala Salarial	Salario Base Profesor Interino Bachiller+80%
Pasos Académicos	8%	2 Pasos (Cada paso vale 4% sobre el Salario Base)
Escalafones	33%	11 escalafones al 3% cada uno hasta Junio 2019
Anualidad	172,50%	32 años de servicio hasta 2019 (30 años a 5,5% y 2 años a 3,75%)
Anualidad Ley 9635	1	
Recargo Funciones	7,50%	Asumir funciones de coordinador de investigación
Zonaje Guanacaste	39%	
Dedicación Exclusiva Docente	30%	

Desglose del salario		Forma de Cálculo
SALARIO BASE DOCENTE	730 153,00	Salario Referencia Profesor Interino Bachiller
PORCENTAJE CATEGORIA ACADEMI(	584 122,00	(+) 80% sobre el Salario Referencia
SALARIO BASE	**1 314 275,00**	
ANUALIDAD	2 380 612,00	Monto congelado de las anualidades adquiridas hasta el año 2019 calculada: (SB de Jul 19 +Pasos Catedráticos+Escalafón+ Fondo Consolidado a esa fecha*160,25%)
ANUALIDAD LEY 9635	26 638,00	Monto nominalizado sobre el Salario Base de Julio 2019, 1 anualidad catedrática vale 26.638
ESCALAFON DOCENTE CONGELADO	459 926,00	Monto congelado de los escalafones adquiridos hasta Junio 2019, calculados: (SB de Enero 19 +Pasos Catedráticos a esa fecha*33%)
FONDO CONSOLIDADO	159 230,00	Derecho adquirido (Escalafones adquiridos en otras categorías)
RECARGO FUNCIONES DOCENTE	140 881,00	7,5% sobre Salario Base+ Pasos Catedráticos+ Escalafón Docente Congelado
PASOS CATEDRATICOS	104 215,00	Monto nominalizado sobre el Salario Base de Julio 2019, 1 paso catedrático vale 52.107,30
DEDICACION EXCLUSIVA DOCENTE	425 547,00	30% sobre Salario Base + Pasos Catedráticos
ZONAJE-GUANACASTE	548 690,00	Monto nominalizado sobre el Salario Base + Pasos Catedráticos de Julio 2019.
SALARIO BRUTO TOTAL	**5 560 014,00**	

Existe en la Universidad de Costa Rica dentro del sector docente, profesores con categorías especiales como los Profesores Invitados, o aquellos que imparten cursos en el Sistema de Estudios de Posgrado que perciben como remuneración un salario contractual, que es establecido por medio de un contrato suscrito por el docente y la administración y no se le aplica ninguno de los conceptos de pago del sistema salarial universitario. En la planilla institucional se encuentran estos salarios con conceptos como:

- Salario Contractual
- Salario Contractual Posgrado, el cual tiene su fundamento en la normativa establecida en la Resolución R-182-2019.

Asimismo, existen los Profesores Invitados o Exbecarios que son asimilados salarialmente a las categorías de Asociado o Catedrático según corresponda, sin embargo, no cuentan con la categoría en régimen académico ni las condiciones de tiempo servido y requisitos de los profesores nombrados en el régimen, por lo cual no pueden considerarse igual a estos, aunque sus salarios consideren los mismos conceptos de pago (Resolución R-4490-2011).

Conforme a lo establecido en el artículo 2 del Reglamento que regula la prestación del Servicio de Personas Funcionarias de la Administración Superior de la Universidad de Costa Rica, se consideran autoridades de la Dirección Superior las personas que dirigen la Rectoría, las Vicerrectorías y las personas miembros del Consejo Universitario.

Adicionalmente, los Lineamientos para la administración y asignación de la carga académica docente del profesorado de la Universidad de Costa Rica, establecen la asignación de carga para puestos directivos dentro de la Universidad, dispuestos en el Estatuto Orgánico, y que tienen algún concepto salarial adicional a los que mantienen en su categoría en Régimen Académico, a saber los siguientes:

1. Decano
2. Director de Sede
3. Director de Recinto
4. Director de Escuela
5. Director de Centro de Investigación
6. Director de Instituto de Investigación
7. Director de Estación Experimental
8. Director de Departamento

Es importante señalar que, para remunerar estos puestos de dirección, se utiliza conceptos de pago propios, calculados como porcentajes de recargo sobre el salario base de la misma escala salarial del sector docente; y quienes ocupan dichos puestos directivos tienen que ser estrictamente profesores en régimen de la Universidad de Costa Rica.

- **Sector administrativo de la Universidad de Costa Rica**

El Reglamento Interno de Trabajo de la Universidad de Costa Rica (Aprobado el 16/10/1969, en la Oficina Legal del Ministerio de Trabajo y Bienestar Social), regula la relación de la ins-

titución con todos sus servidores auxiliares; lo anterior con excepción, del auditor, director administrativo y aquellos cuyo nombramiento debe hacerse mediante elección, conforme con lo establecido en su artículo tres del citado Reglamento

Los servidores administrativos y técnicos, incluyendo los puestos de confianza de la Universidad de Costa Rica, se encuentran cubiertos por un sistema de administración de salarios bajo la administración de la Oficina de Recursos Humanos, tal y como lo dispone el Reglamento de Administración de Salarios de la Universidad de Costa Rica.

Actualmente, la Universidad de Costa Rica en su Manual de Clasificación y Valoración de Clases, denominado Manual Descriptivo de Clases, mantiene para los puestos administrativos de la Institución, un enfoque de clases anchas divididas en los siguientes seis estratos: Dirección (Director y Director Ejecutivo), Mandos Medios (Jefe A y B), Profesional (Profesional A,B,C y D), Especializado (Técnico Especializado A,B,C y D), Asistencial (Técnico Asistencial A y B) y Operativo (Trabajador Operativo A, B y C); cada uno de los puestos indicados tiene asociado un salario base según las clases ocupacionales existentes, y los conceptos de pago asociados a cada persona y puesto.

Ejemplo del Salario Compuesto de un administrativo de la UCR

Detalle de Salario: Director Ejecutivo "RGJ"		
Salario Referencia	Escala Salarial	Salario Base del Puesto
Escalafones	38%	9 escalafones a 4,19% porcentaje de su clase a Diciembre 2019
Anualidad	46,00%	9 años de servicio hasta 2019 (7 años a 5,5% y 2 años a 3,75%)
Anualidad Ley 9635	1	
Remuneración Extraordinaria Adm.	20%	
Incentivo Salarial	15%	
Dedicación Exclusiva Administrativa	30%	

Desglose del salario		**Forma de Cálculo**
ANUALIDAD	519 418,00	Monto congelado de las anualidades adquiridas hasta el año 2019 calculada: (SB de Jul 19 +Escalafón Administrativo a esa fecha*46%)
ANUALIDAD LEY 9635	25 341,00	Monto nominalizado sobre el Salario Base de Julio 2019, 1 anualidad Director Ejecutivo vale 25.341
ESCALAFON ADMINISTRATIVO	402 307,00	Monto congelado de los escalafones adquiridos hasta Diciembre 2019, calculados: (SB de Julio 19*38%)
INCENTIVO SALARIAL	200 752,00	Monto nominalizado sobre el Salario Base de Julio 2019, Incentivo del 15% vale 200.752
REMUNERACION EXT. ADM. (%)	267 669,00	Monto nominalizado sobre el Salario Base de Julio 2019, Rem. Extraordinaria de 20% vale 267.669
SUELDO BASE ADMINISTRATIVO	1 350 257,00	Escala Salarial Vigente
DEDICACION EXCLUSIVA ADMTVA.	405 077,00	30% sobre Salario Base
SALARIO BRUTO TOTAL	**3 170 821,00**	

La Oficina de Contraloría Universitaria desde el año 2001, ha venido alertando sobre la necesidad de ir ajustando y adecuando el sistema salarial universitario a fin de corregir algunas de las debilidades que presenta, por ejemplo:

- Problemas estructurales, metodología del cálculo, complejidad y diversidad de rubros de pago que lo conforman.
- Importancia de los componentes que premian la antigüedad y el acelerado crecimiento vegetativo que se realiza de manera automática.
- Salarios de contratación bajos, para algunas clases ocupacionales.
- Impacto del régimen salarial en los proyectos del vínculo externo al tener una representatividad alta en la estructura de costos.

Hacia el Salario Global en la Universidad de Costa Rica

En el año 2022 se aprobó la Ley General de Empleo Público N°10159 la cual implementa cambios importantes en la gestión de la compensación; a este particular el capítulo VIII, establece los postulados y forma de remunerar a los servidores públicos. En el caso de las personas funcionarias universitarias, la misma ley da la potestad a la institución de construir sus propias columnas salariales globales, sin apartarse de los siguientes postulados:

ARTÍCULO 30- Postulados rectores que orientan la gestión de la compensación. Los salarios de las personas servidoras públicas, a partir de la vigencia de la presente ley, se regirán de acuerdo con los siguientes postulados:

a) El salario será siempre igual para igual trabajo en idénticas condiciones de eficiencia, puesto, jornada y condiciones, independientemente de la institución pública para la que labore.

b) El salario del presidente de la República será el salario más alto de la Administración Pública.

c) La fijación de los salarios se realizará construyendo una metodología de remuneración del trabajo para el servicio público.

d) Cada familia de puestos tendrá una columna de salario global que indicará el puesto y la remuneración que recibirá la persona servidora pública que lo ostente. La columna salarial deberá ser publicada en la plataforma integrada de empleo público.

e) En caso de requerir ajustes o modificaciones a la columna salarial, cuya motivación sea distinta del costo de vida, dicha decisión deberá tomarse de manera fundamentada en criterios técnicos de carácter económico.

f) Los salarios se ajustarán según las reglas contenidas en la Ley 2166, Ley de Salarios de la Administración Pública, de 9 de octubre de 1957.

El Poder Legislativo, el Poder Judicial, el Tribunal Supremo de Elecciones y l**os entes públicos con autonomía de gobierno u organizativa** construirán las respectivas columnas salariales globales de las personas servidoras públicas que desempeñen funciones o labores administrativas, profesionales o técnicas, que sean exclusivas y excluyentes para el ejercicio de las competencias constitucionalmente asignadas.

Para la construcción de esta columna de salarios globales, definido como: remuneración o monto único que percibirá una persona servidora pública por la prestación de sus servicios, establece que la universidad debe especificar una metodología de valoración del trabajo para el servicio público a su cargo; considerando una serie de factores que contarán cada uno con un peso relativo según la contribución al desempeño de los puestos.

Conforme con lo anterior, el Consejo Universitario y la Rectoría de la Universidad implementaron una serie de acuerdos y acciones para dar inicio al cumplimiento de lo dispuesto en la misma, entre ellas:

- A través del acuerdo adoptado por el Consejo Universitario, en el artículo 5 de la sesión n.º 6679, celebrada el 7 de marzo de 2023, se autorizó a la Rectoría a emitir, como medida excepcional, una resolución que definiese un sistema salarial global transitorio para el personal universitario (docente y administrativo) que ingrese a laborar a la Universidad de Costa Rica, a partir del 10 de marzo de 2023.
- Por medio de la Resolución R-81-2023, se establecieron las escalas de salario global transitorio para el sector y docente y administrativo para la remuneración de aquellas personas que ingresen a laborar en la Universidad de Costa Rica, en cualquiera de sus modalidades contractuales de trabajo, a partir de la vigencia de dicha resolución y hasta la aprobación definitiva de la escala salarial global por parte de las autoridades universitarias competentes.
- Mediante el Oficio CU-340-2023, se comunicó el acuerdo tomado por el Consejo Universitario, en la sesión extraordinaria n.º 6683, celebrada el 9 de marzo de 2023, artículos 1 y 2. En dicho acuerdo, se insta a la Rectoría a operacionalizar, vía resolución, lo correspondiente en relación con los puestos declarados como exclusivos, excluyentes y esenciales para el cumplimiento de los fines de la Universidad de Costa Rica como institución de cultura superior.
- Por medio de la Resolución R-41-2023, la Rectoría señaló la exclusión del personal universitario, con respecto a las disposiciones dictadas por el Ministerio de Planificación Nacional y Política Económica, en materia de empleo público. En esa línea, se indicó que la Universidad se encuentra plenamente facultada para construir sus propias familias de puestos y definir su sistema de remuneración de la función pública.
- El Consejo Universitario en sesión n.º 6736, artículo 10, celebrada el 21 de setiembre de 2023, publica en consulta la propuesta de reforma integral a las Regulaciones del régimen salarial académico de la Universidad de Costa Rica.
- Durante la sesión ordinaria n.º 6768 del Consejo Universitario, llevada a cabo el 14 de diciembre de 2023, se aprobó el **Reglamento del Régimen Salarial Académico de la Universidad de Costa Rica**, publicado en La Gaceta Universi-

taria el 3 de enero de 2024, cuyo objetivo es implementar, en el marco de la autonomía universitaria, el principio de salario global en el personal académico y puestos de elección de autoridades universitarias.

- Por medio de la Resolución R-45-2024, la Rectoría establece la escala salarial global definitiva para el sector docente de la Universidad de Costa Rica
- Con Resolución R-116-2024, de fecha 03 de mayo de 2024, la Rectoría de la UCR establece el ámbito de aplicación, mecanismos de traslados, principios rectores y otras reglas de aplicación de la escala de salarial global del personal académico de la institución.
- Por medio de la Resolución R-117-2024, la Rectoría establece las reglas para el traslado de los funcionarios administrativos de la institución al salario global transitorio, según el ámbito de aplicación establecido previamente de forma transitoria, ya que de momento no se ha establecido la escala global permanente para este sector.
- Con Resolución R-863-2025, se establece el Salario Global Definitivo y su aplicación en el sector administrativo, así como el procedimiento de traslado.
- Por medio de la Resolución R-753-2024, se definen las normas de aplicación general para la ejecución del salario global en la Universidad de Costa Rica.

Reflexiones Finales

Ante un cambio de gobierno universitario, criterios encontrados entre autoridades universitarias y panorama incierto sobre la aplicación del salario global respetando el marco de legalidad vigente, pero con la autonomía que constitucionalmente fue asignada a nuestra institución, resulta fundamental que las instancias técnicas presenten reglas claras que logren despejar dudas tales como:

¿Son financieramente sostenibles los nuevos esquemas de remuneración?

¿Hay realmente una igualdad entre personas que realizan las mismas funciones, pero son remuneradas con escalas distintas?

¿Deben estar las regulaciones salariales completamente alineadas a la Ley N°10159?

¿Si tengo derecho a optar por un cambio de esquema salarial, me veré afectado en un futuro?

¿Si me mantengo bajo un esquema de salario compuesto, en algún momento perderé los componentes ya ganados?

¿Cómo serán reconocidos componentes salariales propios de una función dada por ley, bajo una remuneración global?

¿Vale la pena ascender?

¿Cuándo se me reconocerá el salario global definitivo?

… entre muchas otras

OCU BOLETÍN

Seguridad de la Información

MASTER. GUSTAVO ROJAS GARCÍA
Auditor

gustavo.rojas@ucr.ac.cr

I. INTRODUCCIÓN

En términos generales, ¿qué entendemos por "seguridad"?

En un mundo ideal, la seguridad (del latín securitas)[1] la entendemos como "libre o exento de todo peligro, daño o riesgo, o a la confianza en algo o en alguien…". Otra forma de entender la seguridad es por medio de su antónimo: la "inseguridad", que se define como la existencia de un peligro, de un riesgo o que refleja alguna duda sobre un asunto determinado, tales como el robo, delincuencia organizada o accidentes de cualquier tipo, entre otros contextos.

A menudo, la seguridad es denominada como una ciencia interdisciplinaria que se encarga de la identificación, evaluación y gestión de los riesgos a los que se encuentra sometida una persona, organización, un activo o el ambiente. El enfoque principal de la seguridad es la prevención oportuna de los riesgos existentes en el entorno, como requisito para realizar una correcta planificación de los elementos esenciales para implementar un entorno razonablemente seguro.

El término "seguridad" puede tomar diversos sentidos de acuerdo con el área o campo al que haga referencia, así podemos encontrar que existen varios tipos de seguridad, tales como:

- Bioseguridad.
- Seguridad Ciudadana.
- Seguridad Jurídica.
- Seguridad Laboral.
- Seguridad Social.
- Seguridad Vial.
- Seguridad Bancaria.
- Seguridad Física.
- Seguridad de la Información.

¿Qué es la información?

Es importante destacar que el significado de la palabra "información" puede variar según el contexto al que se trate[2]. Para efectos del presente artículo, se entenderá que el término se refiere a un conjunto de datos que, al estar relacionados entre sí, tiene el propósito de generar conocimiento para una persona u organización en particular.

1 Real Academia Española y Asociación de Academias de la Lengua Española (2014). «seguridad». Diccionario de la lengua española (23.ª edición). Madrid: España. ISBN 978-84-670-4189-7.

2 El término "información" es de uso común en prácticamente las Ciencias Biológicas, Sociales y Humanas, la Física, de muchos tipos y clases de Tecnologías, y por supuesto, en nuestra cotidianidad.

En general, la información tiene una estructura interna y puede ser calificada según su significado (semántica), importancia (relativa al receptor), vigencia (en la dimensión espacio-tiempo), validez (relativa al emisor), o por su valor (activo intangible volátil).

¿Qué tipos de información existen?

Existen diversos y variados tipos de información, tales como:

- Información de carácter restringido o privilegiado: Se trata de información de naturaleza sensible que no se comparte públicamente, es decir, está restringida a determinadas personas, grupos u organizaciones. Normalmente, este tipo de información se comparte en reuniones de corte gerencial, políticas o de gobierno. Ejemplos de este tipo de información son los secretos comerciales relacionados con el diseño de nuevos productos y patentes, o bien, los secretos de estado.

- Información de carácter público: Se caracteriza por ser una información accesible a todos los interesados en conocer su contenido. Se publica en cualquier tipo de medio, y en principio, cualquiera puede contar con fácil acceso a ella. Ejemplos de este tipo de información son las noticias de un periódico, un anuncio en televisión, o charla gratuita.

- Información de carácter privado: Este tipo de información está relacionada con la privacidad de los individuos, por ejemplo: las contraseñas bancarias o los documentos propiedad de una empresa. Normalmente, incluso los colaboradores suelen firmar un convenio de confidencialidad con sus patronos para no desvelar ciertos datos de las marcas cuando empiezan a trabajar para ellas.

- Información de carácter externo: Es la información que llega del exterior a determinadas empresas para gestionar algunos temas en concreto. Se utiliza también para valorar a la competencia. Por ejemplo, es el caso en el que llegan datos, o informaciones de competidores presentes en el sector o mercado que provienen de fuentes externas.

- Información de carácter interno: Se trata de aquella que tan solo conoce un grupo de personas. Por ejemplo, la información sobre un proyecto determinado que está trabajando una marca y que un departamento ha de conocer para desarrollar su labor.

A partir de lo mencionado anteriormente, puede notarse que existen muchos tipos de información, no necesariamente se circunscribe al ámbito digital. Un documento impreso propiedad de una empresa pública o privada, grupo o personal, constituye información que podría contar con un valor económico dependiendo de su naturaleza. De igual forma, los secretos industriales, una fotografía, una conversación telefónica, un trozo de papel con datos escritos a mano acerca de un individuo, un audio o video, entre muchos otros, también constituyen información.

II. LA SEGURIDAD DE LA INFORMACIÓN

¿Qué es la Seguridad de la Información?

Por definición, la Seguridad de la Información involucra tres conceptos claves[3], a saber:

- **Confidencialidad:** El concepto de confidencialidad se refiere a que la información debe ser accedida únicamente por los autorizados, y de manera restringida a la información que verdaderamente estos requieran. Se busca prevenir la divulgación no autorizada de información crítica y sensible. Dentro de los aspectos a considerar dentro de la confidencialidad de la información de los individuos, está: su origen racial o étnico, sus convicciones religiosas y espirituales, su estado socioeconómico, información relativa a su salud o vida sexual, antecedentes delictivos, entre otros.

  La confidencialidad es un concepto que tiene mayor utilidad cuando la información ha sido clasificada en las categorías de sensible, restringida o pública.

- **Integridad:** El concepto de integridad de la información, se relaciona con la protección de la exactitud que debe dársele a la información, tanto en su procesamiento como en su almacenamiento. Toda modificación de datos o información deben realizarla los que se encuentran debidamente autorizados, y de manera controlada. Se busca evitar la modificación de información confidencial. La violación de la integridad de la información se presenta cuando un individuo, programa o proceso, ya sea por accidente o con mala fe, modifica, corrompe o borra parte o la totalidad de cierta información.

- Disponibilidad: La información debe estar disponible para quienes cuentan con autorización para accederla, en el momento preciso, en el lugar y de acuerdo con el formato de presentación en que se requiera. Se busca garantizar la continuidad de los servicios sustentada en reglas claras de accesibilidad para los interesados.

III. LA CIBERSEGURIDAD

¿Qué es la Ciberseguridad?

La Ciberseguridad es parte de la Seguridad de la Información, comprende la práctica de defender los activos digitales o informáticos en cualquiera de sus configuraciones[4] en contra de la materialización de eventos no deseados. Puede dividirse, de acuerdo con la empresa Kaspersky[5], en algunas categorías comunes:

3 https://www.iso.org visitada el 11 de setiembre de 2024.

4 Computadoras, servidores, dispositivos móviles, los sistemas electrónicos, redes, Bases de Datos, entre muchos otros.

5 **https://latam.kaspersky.com** visitada el 11 de setiembre de 2024.

- **Seguridad de la Red**. Constituye la práctica de proteger una red informática de los intrusos, ya sean atacantes dirigidos o por software malicioso (también conocido como malware).

- **Seguridad de las Aplicaciones**. Se enfoca en mantener el software y los dispositivos electrónicos y digitales libres de potenciales amenazas. Una aplicación afectada podría brindar acceso a los datos que está destinada a proteger. La seguridad eficaz comienza en la etapa de diseño, mucho antes de la implementación de un programa o dispositivo.

- **Seguridad de los Datos**. Se centra en proteger la integridad y la privacidad de los datos, tanto en el almacenamiento como en su trasmisión de manera segura.

- **Seguridad Operativa**. Incluye los procesos y decisiones para manejar y proteger los recursos de datos. Los permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos se incluyen en esta categoría.

- **La recuperación ante desastres y la continuidad de las Tecnologías de Información (TI)**. Definen la forma en que una organización responde a un incidente de Ciberseguridad, o a cualquier otro evento que afecte la continuidad de las operaciones, se eliminen o publiquen sin autorización datos confidenciales o restringidos.

  Las políticas de recuperación ante desastres, dictan la forma en que la organización restaura sus operaciones e información, para volver a la misma capacidad operativa que existía antes del evento. Esto debe realizarse en el menor tiempo posible y de forma planificada. La continuidad de TI constituye el plan al que recurre la organización, cuando intenta operar sin los recursos que fueron afectados por el incidente.

- La capacitación del usuario final. Aborda el factor de Ciberseguridad más impredecible: las personas. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro. Enseñarles a los usuarios a eliminar los archivos adjuntos de correos electrónicos sospechosos, a no conectar unidades USB no identificadas y otras lecciones importantes es fundamental para la seguridad de cualquier organización.

¿Cuáles son las amenazas a las que se enfrenta la Ciberseguridad?

Las amenazas a las que se enfrenta la Ciberseguridad son básicamente tres:

- **El delito cibernético**. Incluye agentes individuales o grupos que atacan a los sistemas para obtener beneficios financieros o causar interrupciones.

- **Los ciberataques**. A menudo involucran la recopilación de información con fines políticos.

- **El ciberterrorismo**. Tiene como objetivo vulnerar los sistemas electrónicos para causar pánico o temor.

¿Cómo consiguen los delincuentes vulnerar las medidas de Ciberseguridad?

A continuación, se describen algunos de los métodos más comunes utilizados por los delincuentes para vulnerar la Ciberseguridad:

- **Malware.** Se refiere al software malicioso que un criminal ha creado para interrumpir o dañar el equipo de un usuario legítimo. Con frecuencia propagado a través de un archivo adjunto de correo electrónico no solicitado o de una descarga de apariencia legítima, el malware puede ser utilizado por los delincuentes para ganar dinero o para realizar ataques con fines políticos. Existen diferentes tipos de malware, tales como:
    - **Virus**. Es un programa capaz de autorreplicarse, que se incrusta un archivo limpio y se extiende por todo el sistema informático e infecta a los archivos con código malicioso.
    - **Troyanos**. Es un tipo de malware que se disfraza como software legítimo. Los criminales engañan a los usuarios para que carguen troyanos a sus computadoras, donde causan daños o recopilan de manera ilegítima datos confidenciales y sensibles.
    - **Spyware**. Es un programa que recopila, sin que el usuario lo sepa, información confidencial para los delincuentes. Por ejemplo, los detalles de las tarjetas de crédito, y cuentas bancarias entre muchos otros datos sensibles.
    - **Ransomware**. Este malware bloquea el acceso a los archivos y datos de una organización o usuario, con la amenaza de borrarlos, a menos que se pague un rescate.
    - **Adware**. Es software de publicidad que puede utilizarse para difundir malware.
    - **Botnets.** Comprende redes de computadoras con infección de malware que los criminales utilizan para realizar tareas en línea, sin el permiso del usuario u organización.

- **Inyección de código SQL**[6]. Una inyección de código SQL es un tipo de ciberataque utilizado para acceder, robar o modificar datos de una Base de Datos propiedad de una determinada organización. Los criminales aprovechan las vulnerabilidades de las aplicaciones para insertar código SQL, y así lograr su cometido.

- **Phishing**. Consiste en que los criminales atacan a sus víctimas con correos electrónicos, sitios web o llamadas telefónicas, que parecen ser de una fuente legítima, quien de forma sutil les solicita información confidencial. Los ataques de phishing se utilizan a menudo para inducir a que las personas entreguen datos de naturaleza sensible, tales como sus números de tarjetas de crédito y contraseñas, así como otro tipo de información confidencial que debe ser protegida.

- **Ataque de tipo "Man-in-the-middle"**. Comprende un tipo de ciberamenaza en la que un criminal intercepta la comunicación digital entre dos individuos para robar sus datos. Por ejemplo, en una red Wi-Fi no segura, un atacante podría interceptar los datos que se transmiten desde el dispositivo de la víctima y la red.

- **Ataque de denegación de servicio**. Consiste en que los criminales impiden que un sistema informático satisfaga solicitudes legítimas sobrecargando las redes y los servidores con tráfico. Esto hace que el sistema se torne excesivamente lento en sus respuestas, colapse o impide que una organización realice funciones vitales.

¿Cómo defenderse de las ciberamenazas?

A continuación, se presentan algunos consejos de Ciberseguridad:

- **Actualizar el software y el sistema operativo**: esto significa que se aprovecharán las últimas medidas de seguridad disponibles para contrarrestar las amenazas detectadas.

- **Utilizar software antivirus:** las soluciones de seguridad detectarán y eliminarán las amenazas, por esta razón, mantener el software antivirus debidamente actualizado proporcionará un mayor nivel de protección.

- **Utilizar contraseñas seguras**: deben utilizarse contraseñas que no sean fáciles de adivinar.

- **No abrir archivos adjuntos de correos electrónicos de remitentes desconocidos:** los archivos adjuntos podrían estar infectados con malware.

6 Siglas en inglés de Structured Query Language. En español lenguaje de consulta estructurada. Es un lenguaje de dominio específico utilizado en programación, diseñado para administrar, y recuperar información de sistemas de gestión de Bases de Datos relacionales.

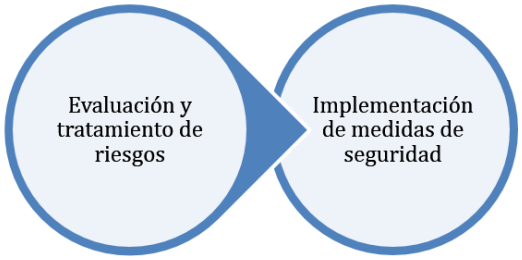
- **No ingresar a sitios de internet maliciosos**.
- **Evitar el uso de redes Wi-Fi no seguras en lugares públicos**: el uso de redes no seguras expone a los usuarios a ataques del tipo “Man-in-the-middle”.

IV. HACIA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) MEDIANTE LA IMPLEMENTACIÓN DE LA NORMA ISO-27001

El eje central de la Norma ISO-27001 es proteger la confidencialidad, integridad y disponibilidad de la información propiedad de una organización pública o privada.

Esto se realiza investigando cuáles son las potenciales amenazas y eventos no deseados que pudieran afectar la información, es decir, a través de la identificación y evaluación de los riesgos, y luego definiendo lo que es necesario implementar para evitar que las amenazas se materialicen, en otras palabras, mediante la mitigación o tratamiento sistemático de los potenciales riesgos[7].

Figura 1



Fuente: https://www.piranirisk.com visitada el 11 de setiembre de 2024.

Las medidas o controles de seguridad a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica. Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, individuos, activos de información, entre otros, dentro de la Norma ISO-27001 se ha detallado cómo integrar estos elementos dentro de un Sistema de Gestión de Seguridad de la Información.

7 Dirección electrónica https://www.advisera.com visitada el 11 de setiembre de 2024.

En la siguiente figura se muestra que la Gestión de la Seguridad de la Información no se limita solamente a la Ciberseguridad, sino que también existen diferentes aspectos que se superponen unos con otros, tales como los procesos de Continuidad del Negocio, y la Gestión y Control de las Tecnologías de Información, todos ellos aspectos relevantes de orden gerencial y organizacional.

Figura 2

Gestión de Riesgos Organizacionales

Fuente: https://www.piranirisk.com visitada el 11 de setiembre de 2024.

Es importante hacer notar que en la figura anterior también incluye la relación existente entre Seguridad de la Información y la Gestión de Riesgos Organizacionales.

Se debe considerar que la Norma 27001:2022 se publicó el 25 de octubre de 2022, y que ya existe una nueva versión: la ISO 27001:2022, que incluye cambios moderados para simplificar su implementación con el propósito de abordar los desafíos de Ciberseguridad

.

V. MARCO JURIDICO Y ESTRATEGICO EXISTENTE

Por su parte Costa Rica, ha respondido a los desafíos del contexto fortaleciendo su marco jurídico y entorno estratégico para fortalecer su ambiente de Seguridad de la Información. Al respecto, destacan las siguientes leyes y estrategias:

- **Ley N° 6683 Derechos de Autor y Derechos Conexos[8]**

  La protección adecuada de la Propiedad Intelectual resulta primordial dentro del entorno globalizado y el uso de las Tecnologías de Información, en donde prevalece la circulación veloz de la información en todos sus formatos y en la que el conocimiento generado en las áreas académica, empresarial, artística, tecnológica o de índole social es cada vez más accesible para un número mayor de individuos, grupos, entidades públicas y privadas.

  El Registro Nacional de Derechos de Autor y Derechos Conexos se ha convertido en una oficina especializada en la materia, con funciones diversas y variadas que van mucho más allá de la registración. De acuerdo con lo estipulado en la Ley N° 6683, las siguientes son funciones del Registro:

  - La registración de las obras artísticas y literarias, así como los actos o documentos relativos a negocios jurídicos de derechos de autor y derechos conexos (contratos, actos de enajenación, etc.)
  - Garantizar la seguridad jurídica de los derechos inscritos con respecto a terceros y dar correcta publicidad de ellos.
  - Fomentar la difusión y el conocimiento sobre los derechos de autor y derechos conexos.
  - Servir de órgano de información y cooperación con los organismos nacionales e internacionales.
  - Orientar y vigilar la utilización lícita de las obras protegidas.
  - Supervisar a las personas naturales o jurídicas que utilicen las obras, interpretaciones, ejecuciones y producciones protegidas.

- **Ley Nº 8968 Protección de la Persona frente al tratamiento de sus datos personales[9]**

  El Artículo 1. Objetivo y fin, indica lo siguiente:

  > "Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes."

8 Decreto Ejecutivo N.º 19117-J-C del 20 de julio de 1989.
9 Diario Oficial La Gaceta, Alcance 287, martes 6 de diciembre del 2016.

Y, el Artículo 2. Ámbito de aplicación, aclara lo siguiente:

> "Esta ley será de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.
>
> El régimen de protección de los datos de carácter personal que se establece en esta ley no será de aplicación a las bases de datos mantenidas por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, siempre y cuando éstas no sean vendidas o de cualquier otra manera comercializadas."

- **Ley Nº 8454, Ley de Certificados, Firmas Digitales y Documentos Electrónicos[10]**

Establece el marco jurídico general para la utilización transparente, confiable y segura en nuestro medio de los documentos electrónicos y la firma digital en las entidades públicas y privadas. Esta ley define la Firma Digital como el conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento.

En su Artículo 1, indica lo siguiente:

> "Que la sociedad de la información y del conocimiento se debe construir sobre la base de la confianza de los ciudadanos y sobre la garantía de la utilización de las tecnologías de la información y las comunicaciones en un doble plano: la protección y confidencialidad de los datos de carácter personal y la seguridad de las transacciones electrónicas."

- **Código Penal. Reforma[11] de los Artículos 196, 196 bis, 230, 293 y 295 y adición del Artículo 167 bis**

El Artículo 196 bis. Violación de datos personales, indica lo siguiente:

> "Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.

10 Diario Oficial La Gaceta 77, de fecha 21 de abril de 2006.
11 Presidencia de la República, San José, 24 de abril de 2013.

La pena será de dos a cuatro años de prisión cuando las conductas descritas en esta norma:

a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

b) La información vulnerada corresponda a un menor de edad o incapaz.

c) Las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.

No constituye delito la publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley.

Tampoco constituye delito la recopilación, copia y uso por parte de las entidades financieras supervisadas por la Sugef de la información y datos contenidos en bases de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley."

El Artículo 230. Suplantación de identidad, establece lo siguiente:

"Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información."

El Artículo 293. Revelación de secretos de Estado, indica lo siguiente:

"Será reprimido con prisión de uno a seis años a quien revele secretos de Estado debidamente decretados relativos a la seguridad interna o externa de la nación, la defensa de la soberanía nacional o las relaciones exteriores de la Republica."

El Artículo 295. Espionaje, señala lo siguiente:

"Será reprimido con prisión de uno a seis años a quien procure u obtenga indebidamente secretos de Estado debidamente decretados relativos a la seguridad interna o externa de la nación, la defensa de la soberanía nacional y las relaciones exteriores de Costa Rica.

La pena será de dos a ocho años de prisión cuando la conducta se realice mediante manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación."

- **Estrategia Nacional de Ciberseguridad de Costa Rica[12]**

  Esta estrategia plantea un esfuerzo conjunto y articulado por el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) entre todos los sectores interesados del país, para garantizar que los objetivos en la materia sean equilibrados, eficaces y acordes con la realidad nacional, definiendo los principios generales que marcarán la pauta país en el campo de la Ciberseguridad. El MICITT contó con el apoyo técnico especializado de la Organización de los Estados Americanos (OEA).

VI. CONCLUSIONES

Lamentablemente, los riesgos que acechan la Seguridad de la Información siguen creciendo aceleradamente en el nivel mundial, tanto en agresividad como en sofisticación, afectando cada vez a un mayor número de individuos, grupos, organizaciones públicas y privadas.

Una clara alerta sobre este hecho, son los datos publicados por la Revista E&N [13] acerca de que: "Costa Rica recibió 882 millones de intentos de ciberataques en 2023, según datos de FortiGuard Labs, el laboratorio de análisis e inteligencia de amenazas de Fortinet. Si se compara la cifra con el año anterior (2.000 millones de intentos de ciberataques en el 2022), es bastante menor, pero reportan que no son buenas noticias". Esta diferencia, probablemente responde al resultado del esfuerzo nacional efectuado para protegerse de las ciberamenaza.

Ante esta perturbadora realidad, las organizaciones y los individuos deben tomar conciencia sobre estar debidamente preparados para enfrentar los riesgos a la Seguridad de la Información, de ahí la enorme importancia de contar con una estrategia integral que permita el monitoreo constante, detección y tratamiento de las amenazas existentes.

Finalmente, conviene indicar que los temas mencionados en este artículo deben ser abordados y analizados oportuna y detenidamente por los individuos y responsables de las organizaciones, dado que el impacto de un evento no deseado, en materia de Seguridad de la Información, además de generar potenciales pérdidas económicas, conlleva graves efectos colaterales, tales como el daño a la buena imagen y pérdida de confianza organizacional.

12 Costa Rica. Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). Estrategia Nacional de Ciberseguridad Costa Rica 2017. – San José, C. R.: MICITT, 2017. ISBN: 978-9968-732-52-9.

13 https://www.revistaeyn.com/tecnologia-cultura-digital/costa-rica-sufrio-882-millones-de-intentos-de-ciberataques-en-2023-FD18395000, visitada el 11 de setiembre de 2024.

OCU
BOLETÍN

Estudio del cumplimiento del régimen de dedicación exclusiva vigente en la Universidad de Costa Rica.Algunas experiencias aprendidas.

MAG. OWEN GOODEN MORALES
Auditor

owen.goodenmorales@ucr.ac.cr

Introducción

El presente ensayo breve, parte la vigencia del régimen de dedicación exclusiva de la Universidad de Costa Rica, por lo que en sus alcances no se encuentran comprendidas consideraciones en torno a los cambios que podrían llegar a materializarse en dicho régimen a partir del contexto de las regulaciones de la Ley Marco de Empleo Público.

Por lo anterior, lejos de pretender agotar los diferentes aspectos y dimensiones que podrían ser considerados a la luz del régimen de dedicación exclusiva vigente en la Universidad de Costa Rica, este ensayo busca exponer algunas de las condiciones de incumplimiento a dicho régimen que son identificadas de forma recurrente por la Oficina de Contraloría Universitaria, ello en aras de que pueda ser considerado de forma preventiva por el segmento de la comunidad universitaria sujeto a éste, así como por aquellas autoridades a quienes corresponde velar por el cumplimiento de las obligaciones del personal a su cargo y que está sujeto a la dedicación exclusiva.

En línea con lo anterior, en el primer apartado se expone una aproximación conceptual a la dedicación exclusiva como figura contractual aplicable en el ámbito de la relación de empleo universitaria, en el segundo apartado se realiza una descripción del fundamento y diligencias de investigación que son ejecutadas por la Contraloría Universitaria en su condición de auditoría interna, tendiente al resguardo de la Hacienda Universitaria. Por último, se detallan algunos supuestos de incumplimiento evidenciados por esta Oficina, los cuales, dada su recurrencia, resulta imperioso que sean conocidos y considerados por las personas funcionarias que optan por sujetarse a las prohibiciones aplicables al formar parte del régimen de dedicación exclusiva.

I. Generalidades del Régimen de Dedicación Exclusiva aplicable en la Universidad de Costa Rica

De manera general, puede afirmarse que la dedicación exclusiva es un régimen laboral facultativo, cuyo origen es contractual, de acuerdo con el cual, la persona funcionaria que es admitida acepta de forma voluntaria cumplir con las prohibiciones que le impone el régimen, en aras de procurar la prestación de sus servicios de forma exclusiva a la Universidad de Costa Rica y a cambio de una compensación económica adicional.

En relación con lo anterior, debe considerarse que la dedicación exclusiva de la Universidad de Costa Rica difiere, en cuanto al origen de su regulación y alcance, de aquella aplicable en otros entes o instituciones públicas[1]. Lo indicado responde al especial régimen de autonomía constitucional que históricamente ha sido reconocido a la Universidad de Costa Rica.

Así las cosas, la dedicación exclusiva en nuestra Institución debe diferenciarse, en especial, de aquellos regímenes que resulten aplicables en otros entes, como los referidos al régimen general aplicable al personal del servicio civil o a las instituciones y empresas públicas cubiertas por el ámbito de la autoridad presupuestaria[2], los cuales, por la cantidad de población que abarcan, suelen ser referidos en pronunciamientos de instancias externas a la Universidad de Costa Rica.

La principal diferencia entre dichos regímenes y el vigente en la Universidad de Costa Rica se encuentra en el alcance de las prohibiciones que imponen, así como la existencia de un listado taxativo de excepciones a dicho régimen prohibitivo.

Precisamente, en el artículo 9 de las Normas que regulan el régimen de dedicación exclusiva en la Universidad de Costa Rica (en adelante NRDE) aprobadas por el Consejo Universitario en sesión N°4706-02 del 20 de marzo de 2002, se regulan tanto las prohibiciones aceptadas en el contrato de dedicación exclusiva que formaliza la Institución con la persona funcionaria, como el listado de excepciones a dichas prohibiciones, excepciones sujetas, en todo caso, a que las actividades exceptuadas no sean realizadas incurriendo en superposición horaria. Lo indicado se detalla en la siguiente tabla.

---

1 Por ejemplo, el artículo 27 del Título Tercero de la Ley N°9635 establece una definición de dedicación exclusiva con alcances diferentes del régimen aplicable a las relaciones de la Universidad de Costa Rica con las personas funcionarias.

2 Dichos regímenes se encuentran regulados en la Resolución DG-254-2009 y sus modificaciones (Normas para la aplicación del Régimen de Dedicación Exclusiva) y el Decreto Ejecutivo N°42266-H (Normas para la aplicación de la dedicación exclusiva para las instituciones y empresas públicas cubiertas por el ámbito de la Autoridad Presupuestaria), respectivamente; ambos ajenos al ámbito universitario.

Tabla N°1

Prohibiciones y excepciones del régimen de dedicación exclusiva en la UCR

Prohibición	Excepción[3]
Ocupar, en otras instituciones o empresas, algún puesto de nombramiento interino o permanente, remunerado o no.	La producción académica de obras de interés institucional y nacional, que genere o no derechos de autor.
Ejercer la profesión en forma independiente, excepto cuando se trate de prestar servicios en forma gratuita para sus necesidades personales, o de su cónyuge, ascendientes, descendientes hasta el tercer grado de consanguinidad o afinidad, siempre y cuando la actividad emanada de dicho interés no conlleve propósitos de lucrar de los familiares aquí mencionados. En estos casos deberá comunicar esta situación a su superior jerárquico.	El ejercicio de funciones de interés institucional en comisiones, asociaciones y juntas directivas de los colegios profesionales o de instituciones educativas nacionales o internacionales, inclusive aquellas que no sean de educación superior, públicas o privadas, culturales, deportivas, científicas.
Dar asesoramiento, remunerado o no, excepto cuando se contraten por medio de la Universidad de Costa Rica con el debido reconocimiento intelectual o económico al interesado.	Las actividades de carácter comunal, remuneradas o no que sean de interés institucional.
Tener bufete, laboratorio, clínica, empresa de asesoramiento, consultorio y cualquier otra actividad similar, o formar parte de ellos.	Las actividades académicas en otras universidades estatales, hasta por un cuarto de tiempo.
	Aquellas actividades que a juicio de la Universidad de Costa Rica se consideren de interés institucional y sean avaladas mediante un convenio o carta de entendimiento.
	Formar parte de no más de dos juntas directivas de sociedades anónimas de conformación familiar, con el propósito de proteger o mantener la unidad de los bienes familiares. La anterior disposición rige también para la participación en fundaciones, asociaciones y cooperativas.

3 En lo referente a aquellas excepciones que requieren una declaratoria de interés institucional, debe considerarse lo regulado en la Resolución de Rectoría R-177-2021 y su reforma por medio de Resolución de Rectoría R-84-2022 que aprueba el Procedimiento para la Gestión de Solicitudes de declaratorias de Interés Institucional

Para acogerse a dichas excepciones, la norma citada establece un procedimiento; a saber, la persona funcionaria debe comunicarlo por escrito a su jefatura inmediata con copia la Oficina de Recursos Humanos, y en el caso del personal docente, con copia a la Vicerrectoría de Docencia. La comunicación debe señalar el tipo de labores que realizará y el periodo y lugar donde las efectuará.

Como se desprende de lo expuesto, las prohibiciones aplicables en el régimen de dedicación exclusiva de la Universidad de Costa Rica van más allá del solo ejercicio de la profesión o profesiones relacionadas con el cargo que ocupa la persona funcionaria, sino que, con el objetivo de garantizar una verdadera dedicación exclusiva de la persona funcionaria, el artículo 9 regula un régimen amplio de prohibiciones por lo que resulta fundamental su conocimiento y valoración por cada una de las personas sujetas al régimen.

II. Control y fiscalización del cumplimiento de las prohibiciones del régimen de dedicación exclusiva

Las acciones de control y fiscalización referentes al cumplimiento de las prohibiciones que impone el régimen de dedicación exclusiva se encuentran a cargo, en primera instancia, de las personas que ostentan la condición de superior jerárquico de las personas sujetas al régimen. Así se encuentra regulado en el artículo 10 de las NRDE, ello es además congruente con lo preceptuado en la Ley General de Control Interno en lo que respecta a los componentes orgánicos del sistema de control interno, por cuanto, éste abarca, además de la auditoría interna, a la administración activa.

Por otro lado, el artículo 11 de las NRDE dispone que la Oficina de Contraloría Universitaria, colaborará con la Administración en la vigilancia y corroboración del cumplimiento de las prohibiciones del régimen. Es precisamente en el marco de dicha disposición que realiza un estudio de monitoreo anual sobre el cumplimiento del régimen de prohibiciones aplicable en materia de dedicación exclusiva.

Como parte de dicho estudio, en su condición de auditoría interna, la OCU realiza las siguientes labores:

1. Se extrae de la planilla institucional aquellas personas que, durante el período que abarca el estudio correspondiente, recibieron el concepto de pago de dedicación exclusiva, considerado éste en sus diferentes denominaciones, según el régimen administrativo o docente al que pertenezca.[4]

4 A partir de la información que consta en las planillas institucionales y normativa universitaria, es posible identificar ocho diferentes denominaciones para el concepto de pago de Dedicación Exclusiva. A manera de ejemplo, en el estudio que abarca el periodo comprendido entre los años 2021 y 2022, se reconoció dicho concepto en más de dos mil casos los cuales son valorados en su totalidad a partir de los supuestos de prohibición y excepción regulados en la normativa.

2. Una vez determinado este grupo, se solicita al Sistema Centralizado de Recaudación de la CCSS (SICERE) que verifique y nos informe cuáles de estas personas es además reportada ante la CCSS por otro patrono adicional a la UCR.

3. Con la información que nos reporta SICERE, se procede al respecto análisis de los resultados obtenidos, pues no siempre implica la existencia de un incumplimiento. A modo ejemplificativo se señalan las siguientes consideraciones que tiene esta auditoría interna al analizar los resultados reportados:

    a) Se nos ha informado casos de personas que son reportadas por el Ministerio de Trabajo y Seguridad Social (bajo los segregados 28 y 30) que corresponden a casos de quienes reciben alguna pensión de algún régimen especial.

    b) También se ha recibido información de funcionarios universitarios que son reportados por la Fundación UCR. Al respecto, debe considerarse que, el convenio marco suscrito entre la UCR y la Fundación UCR establece que las actividades que la Universidad desarrolla por medio de esta fundación son de interés institucional, motivo por el cual, en el tanto no exista superposición horaria, se encuentran exceptuadas del régimen de prohibiciones.

    c) Funcionarios que son adicionalmente nombrados en otras universidades estatales. En este caso la auditoría interna solicita directamente a cada una de las universidades que nos reporten el período y la jornada por la cual las personas se encuentran nombradas, para analizar si la persona se encuentra o no dentro de alguna de las excepciones. Este aspecto será desarrollado en un apartado posterior.

    Del análisis de esta información, suelen surgir situaciones que son reportadas a la Rectoría para la determinación o no del incumplimiento por parte de las personas que son identificadas en este punto.

4. Posteriormente, con base en la misma lista que fue extraída del SIRH, se solicita al Registro Público de Personas Jurídicas nos reporte aquellos casos de personas que estén registradas como parte de la junta directa de alguna sociedad u otras personas jurídicas. La información que se recibe suele ser bastante extensa e implica todo un proceso de análisis para determinar si la persona se encuentra en la excepción establecida en las normas o no. Además, algunos de estos casos reportados por el Registro Público, deben ser revisados ante la Consulta de Situación Tributaria del Ministerio de Hacienda.

El resultado de dichas diligencias de investigación es comunicado a la Rectoría para que, en su condición de contraparte del contrato suscrito con la persona funcionaria, valore si, a partir de las evidencias recopiladas, resulta procedente la resolución del contrato por incumplimiento.

Precisamente el artículo 12 de las NRDE regulan lo concerniente a las consecuencias del incumplimiento de las prohibiciones del régimen; a saber:

i. la resolución del contrato de dedicación exclusiva,

ii. la exclusión del régimen de la persona funcionaria por cinco años y,

iii. el reintegro de las sumas devengadas por concepto de dedicación exclusiva en el periodo de incumplimiento más una indemnización del veinticinco porciento calculado sobre dicho monto.

Con ocasión de un recurso de amparo, la Sala Constitucional valoró la razonabilidad y proporcionalidad de las consecuencias del incumplimiento del régimen de dedicación exclusiva de la Universidad de Costa Rica, dicho tribunal en la resolución N°2642-2000 indicó que:

> En lo que toca a la racionalidad y proporcionalidad de las consecuencias que derivan de la transgresión del sistema de dedicación exclusiva, a juicio de esta Sala, tampoco se suscita enfrentamiento con la Constitución Política. Es cierto que se trata de varias secuelas que se generan con la constatación de un incumplimiento contractual, pero que se explican en las características del régimen y las condiciones y ventajas que de él resultan. Así, la rescisión del contrato, la devolución de los montos percibidos durante la época en que se demostró que se estaba incumpliendo, una multa y la restricción de no ingresar por un período definido temporalmente en el régimen, son efectos que se pueden explicar como sigue: frente al incumplimiento contractual es normal facultar la finalización del acuerdo. Además, obtener la devolución de las prestaciones que una de las partes erogó, sin estar cumpliendo la otra sus obligaciones correlativas. La multa es una típica sanción o carga adicional frente al incumplimiento contractual, lo mismo que la prohibición de suscribir un nuevo contrato por un lapso especificado. Todas estas variantes se relacionan con diferentes reacciones plausibles frente a la inobservancia de obligaciones derivadas de un contrato, de suerte que no resulta irracional ni desproporcionado el que se apliquen conjuntamente.

Sobra indicar que, no son poco frecuentes los casos en los que se evidencian aparentes incumplimientos a las obligaciones contractuales; de ahí que, en el siguiente apartado se detallan algunos de las condiciones de incumplimiento que han sido evidenciadas de forma recurrente por la Oficina de Contraloría Universitaria.

III. Algunos de los principales resultados obtenidos en los estudios en los últimos años

Si bien es conocido el precepto constitucional de acuerdo con el cual nadie puede alegar desconocimiento de las normas jurídicas, y el hecho de que se debe tener conocimiento de las prohibiciones establecidas en el cuerpo normativo aprobado por el Consejo Universitario, no es inusual que ante aparentes incumplimientos de las obligaciones contractuales se alegue desconocimiento sobre el alcance y restricciones que impone la pertenencia al régimen, de ahí que, a continuación se reseñan las condiciones recurrentes de incumplimiento que han sido evidenciadas por la Oficina de Contraloría Universitaria, esto con el fin de que, con carácter preventivo, puedan ser consideradas por el personal universitario y por aquellas autoridades a quienes compete velar por el cumplimiento de las prohibiciones.

a. Personas funcionarias con dedicación exclusiva que además imparten clases en universidades privadas.

El régimen de prohibiciones de dedicación exclusiva aplicable en la Universidad de Costa Rica prohíbe de forma expresa que la persona funcionaria sujeta al régimen ocupe en otras instituciones o empresas, algún puesto con independencia de su carácter temporal o permanente, remunerado o no. Asimismo, en lo que respecta a las universidades privadas, las excepciones previstas no contemplan la posibilidad de realizar actividades académicas en estos centros privados de enseñanza superior.

Como se detallará en el punto siguiente, la excepción aplicable para realizar actividades académicas en instituciones de educación superior públicas no es extensiva a las relaciones que el personal universitario pueda mantener con universidades privadas.

b. Personas funcionarias con dedicación exclusiva y con jornadas superiores al cuarto de tiempo completo en otras universidades de CONARE.

La posibilidad de desarrollar actividades académicas en otras universidades estando sujeto al régimen de dedicación exclusiva de la Universidad de Costa Rica, solo resulta válida cuando se trata de nombramientos en universidades estatales.

Dicha excepción solo habilita una dedicación máxima de un cuarto de tiempo completo en las universidades estatales diferentes a la UCR y exclusivamente para el desarrollo de actividades académicas.

Sobre este particular, debe considerarse que, si bien el artículo 41 del Convenio de Coordinación de la Educación Superior Universitaria Estatal en Costa Rica regula como jornada máxima en el sector público para el personal universitario por hasta un tiempo y medio[5] y en igual sentido se encuentra el Reglamento de dicho artículo, dicho límite se ve reducido en el caso del personal de la Universidad de Costa Rica que cuenta con dedicación exclusiva, ya que, como se indicó, este régimen solo admite como excepción el nombramiento en otras universidades estatales hasta por un cuarto de tiempo.

Cabe destacar que, la excepción referida, únicamente habilita el desarrollo de actividades académicas en instituciones de educación superior universitarias, y que la jornada máxima debe ser considerada en cada caso por la persona docente en coordinación con la universidad en la que pretende prestar sus servicios de forma concomitante a su pertenencia al régimen de dedicación exclusiva en la UCR, ya que ello dependerá de la jornada laboral vigente en dichas instituciones, garantizando que el nombramiento que mantendrá no supere el cuarto de tiempo completo establecido como máximo para la excepción.

c. Funcionarios universitarios con dedicación exclusiva que pertenecen a dos o más juntas directivas de personas jurídicas u ocupan puestos en estas entidades

En Costa Rica se extendió la práctica de constituir personas jurídicas, en especial sociedades mercantiles, con el único fin de mantener bienes que conforman el patrimonio familiar, esto a pesar de que dichas entidades no desarrollan actividad empresarial en su conceptualización técnica[6], entendida como aquella Agrupación organizada que se dedica —de forma profesional, habitual y continua— al intercambio de bienes y servicios, mediante la reventa o intermediación; o en la transformación de materias para la creación y venta de productos (Salazar, 2020), o aquella Actividad económica organizada para producir bienes o prestar servicios destinados al mercado (Real Academia Española, 2023).

Como parte de su estructura organizativa, las sociedades constituidas según el Código de Comercio mantienen juntas directivas u órganos equivalentes, así como puestos de las personas a cargo de la administración y representación

5 ARTÍCULO 41: Ningún servidor de las Instituciones signatarias podrá desempeñar otro puesto con superposición horaria, ni trabajar en Instituciones Estatales más de tiempo y medio. La violación de lo aquí dispuesto será justa causa de despido del servidor, si dentro del término que se conceda para que se regularice su situación, no lo hiciere.

6 De conformidad con la definición de comerciante establecida en el artículo 5 del Código de Comercio, y las diferencias entre estas según cada uno de los incisos que lo componen, la condición de comerciante no implica necesariamente que un comerciante, en sentido formal, realice actividad empresarial. Esta última fue definida por la Sala Primera en la Resolución 7-1994, en donde señaló que: "…el empresario cumple un papel intermediario entre quienes ofrecen en el mercado capital y trabajo y aquellos que demandan bienes o servicios…".

de las entidades. Por lo anterior, y precisamente considerando el alcance del régimen de prohibiciones aplicable a la dedicación exclusiva en la UCR, el cual, como fue expuesto, prohíbe ocupar cargos en otras instituciones o empresas, el Consejo Universitario, mediante reforma aprobada en sesión N°5736-04 del 27 de junio de 2013, incorporó como excepción a las prohibiciones del régimen la posibilidad de formar parte de no más de dos juntas directivas de personas jurídicas de conformación familiar y con el fin de proteger o mantener la unidad de los bienes familiares.

De forma recurrente, la Oficina de Contraloría Universitaria, ha evidenciado casos en los que el personal sujeto a dedicación exclusiva ocupa cargos en más de dos personas jurídicas de forma concurrente a su pertenencia al régimen, con lo cual se excede el máximo habilitado por la excepción referida.

Por otro lado, también se ha identificado personal con dedicación exclusiva, quienes ocupan puestos en personas jurídicas que desarrollan actividades empresariales de diversa índole, con lo que, al igual que en el caso anterior, se incumple los presupuestos regulados para la aplicación de la excepción.

Sobre este tema, debe recordarse que el artículo 9 de las NRDE, con la salvedad dicha de las excepciones expresamente admitidas, estable una prohibición general para que el personal universitario sujeto al régimen ocupe cargos o nombramientos en otras entidades, con independencia de sus condiciones de temporalidad o no y remuneración o gratuidad; de ahí que, los nombramientos en personas jurídicas en puestos que no son de junta directiva, pueden de igual forma implicar un eventual incumplimiento a las prohibiciones del régimen.

d. Funcionarios universitarios con dedicación exclusiva reportados a la CCSS en planilla de un patrono diferente a la UCR.

Resulta también recurrente la verificación de personal con dedicación exclusiva que, de forma concurrente a su pertenencia al régimen, es reportada en planilla de otros patronos.

Como se ha expuesto, el alcance de las prohibiciones imposibilita que las personas funcionarias que forman parte del régimen ocupen algún otro puesto en instituciones o empresas, públicas o privadas, de forma temporal o permanente, sean las labores remuneradas o no. Asimismo, el mismo artículo 9 de las Normas que regulan el régimen establecen un listado taxativo de excepciones a las prohibiciones allí reguladas, por lo que en casos en los que las personas funcionarias son reportadas en planilla de otros patronos se verifica si se encuentran en un supuesto de excepción, caso contrario se procede con el informe correspondiente para la adopción de las medidas aplicables por parte de la Rectoría.

Conclusión:

A pesar de que el régimen de dedicación exclusiva atraviesa una coyuntura de cambio, al amparo de la normativa aplicable, los contratos suscritos mantienen vigencia, por lo que resulta oportuno y necesario considerar los aspectos aquí señalados, referidos a los resultados del monitoreo del cumplimiento de sus prohibiciones.

Sobre el particular, resulta especialmente relevante considerar que la dedicación exclusiva en la Universidad de Costa Rica implica un régimen de prohibiciones amplio, que limita más allá del ejercicio de la profesión o profesiones vinculadas con el cargo de la persona funcionaria sujeta al régimen. Asimismo, la adecuada valoración del listado de excepciones a las prohibiciones que implica el régimen constituye el aspecto de mayor incidencia en la eventual determinación de incumplimientos al régimen, de ahí la importancia de que siga el procedimiento para acogerse a las excepciones y, con carácter precautorio, se realicen las consultas previas ante las instancias competentes, con el fin de evitar las consecuencias de un eventual incumplimiento.

Referencias:

Normativa

- Normas que regulan el régimen de dedicación exclusiva en la Universidad de Costa Rica. Aprobadas por el Consejo Universitario en sesión N°4706-02 del 20 de marzo de 2002. Publicadas en la Gaceta Universitaria 2-2002 del 4 de abril de 2002.
- Convenio de Coordinación de la Educación Superior Universitaria Estatal en Costa Rica. Ratificado por el Consejo Universitario en sesiones 2885-02 y 2887-17 del 30 de marzo de 1982 y 13 de abril de 1982, respectivamente. Publicado en Leyes, Convenios y Decretos de la Educación Superior Universitaria Estatal en Costa Rica de CONARE.
- Reglamento al artículo 41 del Convenio de Coordinación de la Educación Superior Universitaria Estatal en Costa Rica. Ratificado por el Consejo Universitario en sesión 3390-17 del 29 de julio de 1987. Publicado en La Gaceta Universitaria 23-87 del 21 de agosto de 1987.
- Código de Comercio, Ley N°3284 del 30 de abril de 1964. Aprobado por la Asamblea Legislativa de la República de Costa Rica. Publicado en la Gaceta N°119 del 27 de mayo de 1964.

Resoluciones judiciales

- Sala Constitucional de la Corte Suprema de Justicia. Resolución N°2642-2000.
- Sala Primera de la Corte Suprema de Justicia. Resolución N°7-1994.

Páginas web

- SALAZAR CARVAJAL, Pablo. (2020). Diccionario usual del Poder Judicial. Poder Judicial, Costa Rica. https://diccionariousual.poder-judicial.go.cr/index.php/diccionario empresa, tomada el 17 de julio de 2024.
- Real Academia Española. Diccionario panhispánico del español jurídico, 2023. https://dpej.rae.es/dpej-lemas/empresa

OCU
BOLETÍN

Importancia de la Gobernanza de Datos Institucionales en los Procesos de Auditoría Interna

M.I.I MARCO MONGE VÍLCHEZ
Director Oficina de Registro UCR

marco.monge@ucr.ac.cr

La evolución constante de las tecnologías de la información ha generado una creciente dependencia en los sistemas de información. En el pasado, las limitaciones estaban relacionadas con el almacenamiento y procesamiento de datos, elementos que han perdido relevancia con el desarrollo de nuevas capacidades tecnológicas. Actualmente, los mayores retos en la gestión de la información se encuentran en el desarrollo e implementación de un modelo de gobernanza de datos que permita conocer la importancia del ecosistema proceso-sistema-usuario, de modo que se permita conocer la gestión sustantiva universitaria (docencia, investigación y acción social) y la gestión administrativa con el objetivo de generar valor público, considerando los principios de eficacia, eficiencia y efectividad.

Existe una frase atribuida a William Thomson (Lord Kelvin), un destacado físico y matemático, que dice así: "Lo que no se define no se puede medir. Lo que no se mide, no se puede mejorar. Lo que no se mejora, se degrada siempre". Esta perspectiva enfatiza la necesidad del análisis de datos como una herramienta indispensable para la optimización continua de los procesos. La adecuada gestión del ecosistema de datos es esencial para avanzar en la gestión institucional y, en consecuencia, en la efectividad de la auditoría interna.

Conceptos Generales

Antes de definir requerimientos y modelos de gobernanza de datos, es necesario conocer las siguientes definiciones:

- **Gobernanza**: "todos los procesos de gobierno, instituciones, procedimientos y prácticas mediante los cuales se deciden y regulan los asuntos que afectan al conjunto de la sociedad" (Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, s.f.).

- **Datos:** un dato es un conjunto de factores objetivos sobre un hecho real, definido en un contexto empresarial como un registro de transacciones. Por sí mismo tiene poca o ninguna relevancia o propósito, ya que requiere de análisis para ser convertido en información y/o conocimiento que favorezca y fundamente las decisiones organizacionales (Davenport & Prusak, 1999, como se cita en Carrión, 2017).

- **Valor de los datos:** es la capacidad que tienen los datos para brindar beneficios significativos a las organizaciones, como impulsar la innovación, mejorar la toma de decisiones y optimizar las operaciones. Si los datos se manejan correctamente, pueden aumentar la productividad y ofrecer nuevas oportunidades para las organizaciones. Las organizaciones pueden utilizar estos datos para obtener información valiosa y mejorar constantemente sus prácticas operativas gracias a la tecnología actual (Hewlett Packard Enterprise, s.f.).

- **Gobernanza de datos:** Microsoft Azure, define la gobernanza de datos como el conjunto de procesos, directivas, roles, métricas y normas que aseguran el uso eficaz y eficiente de la información, además de establecer procesos que mantengan los datos seguros, privados, precisos y utilizables durante su ciclo de vida.
- **Sistemas de información:** Gonzalez-Longatt describe los sistemas de información como herramientas tecnológicas que permiten el registro, almacenamiento y difusión de datos, así como la formulación de conclusiones a partir de estos.
- **Interoperabilidad:** se define como la capacidad de aplicaciones y sistemas para intercambiar datos de manera segura y automática, superando barreras organizativas, políticas y geográficas. Esta capacidad es fundamental para permitir la comunicación en tiempo real entre múltiples sistemas y departamentos, imprescindible para las necesidades institucionales y por ende para los procesos de auditoría. La interoperabilidad incluye mecanismos, estándares, protocolos y tecnologías que facilitan el flujo de datos entre sistemas sin intervención humana, mejorando la eficiencia y calidad de los servicios organizacionales (Amazon Web Services, s.f.). Este es un principio esencial para que los sistemas de auditoría puedan interoperar con los diversos sistemas institucionales.

La Importancia de los datos

En la actualidad, para cualquier organización, los datos son uno de los activos más valiosos en la era digital. Las empresas pueden innovar, mantener una ventaja competitiva y tomar decisiones informadas si tienen la capacidad y habilidad de recopilar, analizar y utilizar datos de manera efectiva. Los datos permiten entender mejor las operaciones internas, el comportamiento de los clientes, ventas entre otros, que ayuda a identificar oportunidades y reducir riesgos.

En el ámbito de la auditoría, los datos son esenciales para evaluar y mejorar la eficiencia de los procesos organizativos. Una auditoría se basa en la recopilación y análisis de datos para asegurar que las políticas, normativas, reglamentos y procedimientos se cumplan correctamente, además de identificar áreas que requieren mejoras. En este sentido, la gobernanza de datos desempeña un papel significativo al garantizar que los datos utilizados sean precisos, completos y confiables, lo que permite tomar decisiones basadas en evidencia real y sólida.

A continuación, se muestran algunos ejemplos donde se utilizan los datos en el análisis de la gestión, que incluyen:

- **Financieros y contables:** en este contexto, los datos son utilizan para verificar la exactitud de los registros financieros. Se comparan los datos reales con los datos registrados en los libros contables para detectar diferencias y/o fraudes. Por ejemplo, se comparan los ingresos registrados en los libros contables con los datos reales (como los recibos de ventas, facturas por pagos de servicios, transferencias, entre otros) para detectar discrepancias o posibles fraudes.

- **Operativos:** los datos se emplean para medir la eficiencia de los procesos y la utilización correcta de los recursos públicos. Por ejemplo, en un servicio universitario, se recopilan datos sobre la duración del servicio, la cantidad de servicios brindados y los recursos utilizados (humanos, económicos, materiales). Estos datos ayudan a identificar áreas de mejora y optimización.

- **Cumplimiento (normativa):** en este aspecto, los datos se utilizan para asegurar que los procesos institucionales se ajusten a las normativas y políticas que la regulan. Por ejemplo, verificar las jornadas laborales respecto al Código de Trabajo.

Modelo de Gobernanza de Datos

El modelo de gobernanza de datos se refiere a los procedimientos, estructuras y políticas que garantizan que los datos sean administrados de manera ética y efectiva en una organización o en un contexto particular, como el sector público. Los elementos regulatorios relacionados con la disponibilidad y el uso de los datos, así como la organización, la integración e interoperabilidad del ecosistema de datos, forman parte de este modelo (Cabello, 2023)

Aunque los sistemas de información y la gobernanza de datos puedan parecer conceptos similares, en realidad hay una diferencia importante: los sistemas de información están diseñado para satisfacer las necesidades particulares de un departamento o de una organización. En contraste, la gobernanza de datos es un concepto más amplio que abarca los principios, políticas y prácticas utilizadas para la gestión de datos en toda la organización.

A continuación, se definen los principales elementos que debe tener un modelo de Gobernanza de Datos:

A) **Ciclo de vida de los datos**

Constituye la trayectoria que atraviesa un dato desde su creación hasta su eliminación o archivado. Comienza con la obtención o generación de los datos, sigue con su procesamiento y almacenamiento, y abarca su uso para diversas aplicaciones. Además, incluye la capacidad de compartir los datos con otros sistemas o personas. Finalmente, cuando los datos ya no son necesarios, se procede a su eliminación o archivado. El ciclo de vida de los datos es fundamental para garantizar una gestión adecuada y eficaz de los datos a lo largo de su existencia.

Según Cabello (2023), el ciclo de vida de los datos está compuesto por:

- **Creación/Captura:** se refiere a la obtención, generación o modificación inicial de los datos.
- **Procesamiento:** incluye la limpieza, tratamiento y transformación de los datos para estandarizarlos y prepararlos para su uso.
- **Almacenamiento:** existen diversas formas de almacenar datos, como en data warehouses, data lakes, entre otros.
- **Uso/Reutilización:** implica la aplicación de los datos en actividades como inteligencia artificial, minería de datos y análisis estadísticos.
- **Intercambio/Publicación:** se refiere a la interoperabilidad entre diferentes instancias institucionales y al producto final de los datos utilizados.
- **Eliminación/Archivado:** comprende la supresión controlada de datos que ya no son necesarios y su archivo seguro para referencia futura si corresponde.

B) **Alianzas y Enfoques Colaborativos**

En el ámbito de la auditoría, colaborar con otras instancias universitarias, autoridades y expertos externos es clave. Esto permite aprovechar datos y recursos, mejorando la precisión y eficiencia del proceso. Trabajar juntos ayuda a resolver problemas y encontrar soluciones innovadoras, haciendo que la auditoría sea más efectiva y completa.

C) **Gestión de los datos:**

La recopilación, conservación y el uso de datos de manera efectiva, segura y económica se conoce como gestión de datos. La gestión de los datos tiene como finalidad ayudar a individuos, organizaciones y dispositivos conectados a utilizar los datos de manera óptima dentro de los límites de las regulaciones y las políticas, para ello, es fundamental tener una estrategia sólida de gestión de datos en la actualidad debido a la creciente dependencia de activos intangibles para generar valor (Oracle, s.f.).

Modelo de Datos en la Auditoría

Considerando lo mencionado previamente, un modelo de datos se puede definir como un esquema organizativo que establece la forma en que se estructuran, almacenan y gestionan los datos necesarios para llevar a cabo auditorías de manera efectiva. Este modelo tiene como objetivo asegurar que los datos permanezcan organizados y accesibles, definiendo directrices para su administración y los controles necesarios para proteger la información.

D) **Acceso a bases de datos:** el acceso a los datos implica la capacidad de recuperar y utilizar la información almacenada en bases de datos o sistemas de almacenamiento. Según (Hewlett Packard Enterprise, s.f.), el propósito del acceso a los datos es permitir a individuos y organizaciones extraer y utilizar datos almacenados en repositorios, facilitando su uso en una variedad de aplicaciones.

Un acceso eficiente a las bases de datos permitirá a los auditores obtener la información necesaria de manera rápida y precisa para realizar las revisiones necesarias.

E) **Extracción de Datos**: "La extracción de datos es el proceso de recuperar o extraer datos de diversas fuentes y convertirlos a un formato utilizable y significativo para su posterior análisis, generación de informes o almacenamiento. Es uno de los pasos más importantes en datos de gestión que le permite introducir datos en aplicaciones o análisis posteriores" (Astera Equipo de Análisis, 2024).

Extraer los datos precisos de manera efectiva asegura que la auditoría basará sus informes y recomendaciones en información actualizada y pertinente.

- **Procesamiento y análisis:** mientras que el procesamiento de datos implica transformar datos sin procesar en información valiosa para las empresas (Astera Equipo de Análisis, 2024), el análisis de datos, según (Amazon Web Services, s.f.), se trata de convertir los datos sin procesar en información práctica mediante el uso de herramientas, tecnologías y procesos para encontrar tendencias y resolver problemas mediante datos.

  El análisis y procesamiento de datos permite identificar patrones, anomalías y áreas de mejora, proporcionando una base sólida para las sugerencias y recomendaciones de la auditoría.

- **Visualización:** la visualización de datos consiste en emplear gráficos, infografías y mapas para convertir datos complejos, extensos o numéricos en representaciones visuales más comprensibles. Este método facilita el análisis y la interpretación de la información, haciendo que sea más accesible. Las herramientas de visualización optimizan y automatizan esta tarea, asegurando una comunicación precisa y detallada, lo que permite extraer conocimientos útiles a partir de datos sin procesar (Amazon Web Services, s.f.).

  Como parte final de este proceso, la visualización permite mostrar los resultados de forma clara y entendible para compartir los hallazgos y recomendaciones a las partes interesadas.

  En este contexto, para asegurar que los datos estén bien organizados y sean accesibles a lo largo de todo el proceso, se debe tener un modelo de datos cuidadosamente diseñado en la auditoría. Este modelo facilita una auditoría exacta y minuciosa al integrar de manera eficiente el acceso, la extracción, el análisis, procesamiento y la visualización de los datos. De esta manera, se mejora la calidad de los informes y se facilita la identificación de riesgos, el cumplimiento de normativas y la generación de recomendaciones que generen valor público.

Retos y desafíos

Conocer y mejorar la gobernanza de datos es relevante para la auditoría interna: el éxito de los procedimientos de auditoría interna depende de un modelo de gobernanza de datos funcional. Para una evaluación efectiva de la eficiencia de la organización, este modelo garantiza que la información sea accesible, organizada y precisa. Sin un modelo de gobernanza específico, la confiabilidad de los datos utilizados en las auditorías se ve comprometida; esto tiene un impacto en la calidad y aplicación de sus recomendaciones.

Garantizar la interoperabilidad entre varios sistemas y promover la cooperación entre instancias universitarias es fundamental para maximizar la eficiencia y precisión de la gestión universitaria y por ende del trabajo de la auditoría interna. La cooperación efectiva y la capacidad de intercambiar datos de manera segura y automática facilitan la recopilación, el análisis y la presentación de datos. Esto fomenta una gestión de datos más efectiva y una toma de decisiones más informada, además de mejorar la precisión de las auditorías.

Para concluir, el modelo de gobernanza de datos resulta importante para la eficacia de las auditorías internas, ya que asegura que la información sea precisa, bien organizada y accesible. Dada la evolución tecnológica y la creciente importancia de los datos, es esencial adoptar un enfoque estructurado en su gestión. Un modelo de gobernanza adecuado permite realizar auditorías más precisas y fundamentadas, facilitando una toma de decisiones más informada. Además, la promoción de la interoperabilidad entre sistemas potencia esta efectividad, contribuyendo así al valor público y a la mejora continua de las organizaciones.

Bibliografía

Amazon Web Services. (s.f.). ¿Qué es la interoperabilidad? Obtenido de https://aws.amazon.com/es/what-is/interoperability/#:~:text=La%20interoperabilidad%20se%20refiere%20a,compartan%20informaci%C3%B3n%20en%20tiempo%20real.

Amazon Web Services. (s.f.). Amazon Web Services. Obtenido de https://aws.amazon.com/es/what-is/data-analytics/

Amazon Web Services. (s.f.). Amazon Web Services. Obtenido de Amazon Web Services: https://aws.amazon.com/es/what-is/data-visualization/

Astera Equipo de Análisis. (24 de Julio de 2024). Astera. Obtenido de https://www.astera.com/es/type/blog/what-is-data-extraction-a-brief-guide/

Astera Equipo de Análisis. (02 de Abril de 2024). Astera. Obtenido de https://www.astera.com/es/knowledge-center/what-is-data-processing-definition-and-stages/

Cabello, S. (2023). Análisis de los modelos de gobernanza de datos en el sector público: una mirada desde Bogotá, Buenos Aires, Ciudad de México y São Paulo. Santiago de Chile: Comisión Económica para América Latina y el Caribe (CEPAL).

Carrión, J. (2017). Universidad Nacional Autónoma de México (UNAM). Obtenido de Universidad Nacional Autónoma de México (UNAM): https://iibi.unam.mx/voutssasmt/documentos/dato%20informacion%20conocimiento.pdf

Gonzalez-Longatt, F. M. (s.f.). Universidad Veracruzana. Obtenido de Universidad Veracruzana: https://www.uv.mx/personal/artulopez/files/2012/08/FundamentosSistemasInformacion.pdf

Hewlett Packard Enterprise. (s.f.). Hewlett Packard Enterprise. Obtenido de Hewlett Packard Enterprise.: https://www.hpe.com/lamerica/es/what-is/value-of-data.html#:~:text=El%20valor%20de%20los%20datos%20se%20refiere%20a%20los%20beneficios,y%20nuevos%20flujos%20de%20ingresos.

Microsoft Azure. (s.f.). Microsoft Azure. Obtenido de Microsoft Azure: Microsoft Azure. (n.d.). Definición de gobernanza de datos. Azure. https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-a-data-governance/#:~:text=La%20definici%C3%B3n%20de%20gobernanza%20de,y%20eficiente%20de%20la%20informaci%C3

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (s.f.). Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Obtenido de Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos: https://www.ohchr.org/es/good-governance/about-good-governance#:~:text=El%20concepto%20de%20gobernanza%20hace,al%20conjunto%20de%20la%20sociedad

Oracle. (s.f.). Oracle. Obtenido de Oracle: https://www.oracle.com/es/database/what-is-data-management/

OCU
BOLETÍN

Evaluación del riesgo de control interno

LIC. JORGE PADILLA ZUÑIGA
Jefe Oficina de Suministros UCR

jorge. padilla@ucr.ac.cr

En la actualidad, las entidades públicas y privadas están inmersas en un entorno impredecible, competitivo e inestable, que incrementa los niveles de riesgo en todas las actividades y estratos de la estructura orgánica y, por consiguiente, presentan retos para los cuales deben estar preparadas.

La vigencia de las entidades y su gestión exitosa estriba en la capacidad para anticipar los riesgos y tomar las previsiones adecuadas y oportunas; o bien, afrontarlos y adaptarse lo mejor posible a los escenarios que se presenten.

El proceso de evaluación y gestión de riesgos es, sin lugar a duda, una de las diversas herramientas en que pueden apoyarse las entidades para lograr una alineación adecuada entre el cumplimiento de los objetivos institucionales y las amenazas, contingencias e inestabilidades imperantes en el entorno particular.

"La evaluación de riesgos es un proceso dinámico e interactivo orientado a identificarlos y gestionarlos para garantizar la consecución de los objetivos."

Pero, porqué actualmente hablamos tanto de riesgos y control interno si en la administración estos términos han sido acuñados por mucho tiempo. Para entenderlo es importante retrotraerse a 1985 en los Estados Unidos, año en que se presentaron diversos acontecimientos, debido a las malas prácticas por parte ciertas entidades que generaron una crisis en el sistema financiero de esa época. Esto motivó a que cinco organizaciones que, preocupadas por los sucesos, conformaran el denominado Comité de Organizaciones Patrocinadoras de la Comisión Treadway, en procura de realizar estudios de los factores que llevaron a las empresas a la presentación de información financiera fraudulenta. Con los elementos recabados, elaboraron un informe con recomendaciones en materia de control interno, que ha sido referente para todo tipo de entidades.

Este análisis objetivo e independiente que hizo este Comité sobre los orígenes y las consecuencias de los acontecimientos que se venían suscitando, han hecho que el marco de referencia propuesto sea una herramienta imprescindible para el cumplimiento de los objetivos trazados por las entidades.

Entorno competitivo de las entidades públicas y privadas

Los medios de comunicación saturan nuestros sentidos con ofertas de toda naturaleza, productos de diferentes precios y calidades, innovaciones y una gran gama de artículos y servicios para escoger, según posibilidades económicas, creencias gustos y preferencias. Lo difícil es discernir a cuál información debemos prestar atención y cuál desechar, situación que vuelve inestable los deseos o necesidades de los usuarios o clientela.

El mercado en todas las áreas se ha vuelto mucho más competitivo, ya no es aquel en el que dependíamos de una empresa, servicio o producto, sin el cual nuestras actividades podían verse limitadas, o por lo menos así lo percibíamos. Tanto es así que perdemos la perspectiva si un producto deja de ser bueno, o simplemente aceptamos otro que el mercado nos ofrece por su tecnología, funcionalidades o facilidades.

En este mercado tan competitivo, cada ente, público o privado, debe valorar las fortalezas y oportunidades, pero, ante todo, determinar cuáles son sus riesgos internos y externos que pueden afectar el logro de los objetivos que se ha trazado. Debe estar atento al giro de negocio, a la competencia, los cambios económicos, regulatorios, de mercado, entre otros. La historia nos presenta muchos ejemplos de empresas que no evaluaron, con la rigurosidad que requería, los riesgos que se venían presentado.

En la actualidad, los estudiantes que recién ingresan a la universidad probablemente nunca han escuchado de empresas como Kodak o Nokia, pero a finales de los años 90 e inicios del 2000 eran marcas que estaban en nuestra vida diaria. Quién no deseaba una cámara Kodak o un Nokia 1100, el teléfono móvil más vendido en esa época.

Detengámonos un momento y veamos el caso de Kodak, la empresa con más patentes de investigación e innovación registradas que, incluso, en 1975 desarrolló la cámara digital, con una cinta que guardaba hasta 30 fotos en el increíble lapso de 23 segundos, algo nunca visto en esa época. Sin embargo, sus ejecutivos restaron importancia a los riesgos de su negocio, pese a que los conocían y tomaron decisiones erróneas, como la venta de otras inversiones lucrativas para dedicarse a su core bussiness, que en esa época era la fotografía y el revelado. Perdieron la oportunidad de explotar lo que a la postre sería el negocio del futuro, la cámara digital.

Esa enorme transnacional, con representación en múltiples países del mundo, con un centro de investigación e innovación, restó importancia a que empresas como Apple, Sony, Google y Fuji Film que, usando incluso muchos de sus inventos, se posesionaron de un mercado con productos que eran propios de sus investigaciones debidamente patentizadas. Esas decisiones los llevaron al punto de tomar acciones desesperadas, como la venta de cerca de 1100 patentes en las ridícula suma de $525 millones para evitar su quiebra.

Un rumbo no muy distinto tuvo la empresa finlandesa Nokia, que tampoco determinó los riesgos que le presentaba el entorno. Esta empresa dominó el mercado de los teléfonos móviles en la segunda mitad de los años 90 e inicios de los años 2000, introduciendo al mercado el primer teléfono móvil en el año 1992, y el primer teléfono con cámara digital, con las mayores ventas en el mundo en el año 1998.

No obstante, no visualizó que la tecnología táctil era el futuro y, por tanto, siguió apostando a que su negocio de telefonía debía dirigirse a reducir costos y mantener sus ventas; o bien, podríamos presumir por el desenlace, que no evidenciaron riesgos asociados a sus decisiones. En consecuencia, lo que era un negocio sumamente lucrativo, fue superado por otras marcas, conduciéndolos inevitablemente a vender los derechos de telefonía móvil a Microsoft.

Ahora bien, las empresas e instituciones públicas no están exentas de enfrentarse a riesgos que pueden afectar su propósito o giro de actividad, pero con el agravante de que no son los accionistas o inversionistas los más afectados, si no la sociedad que espera de sus servicios. En la actualidad, los entes públicos se desarrollan en un contexto dinámico, incierto y de diferente naturaleza e intensidad que, sin lugar a duda, repercuten en su sistema de gestión y en el logro de los objetivos. La naturaleza de tales eventos hace que estas instituciones deban identificar y evaluar constantemente el conjunto de riesgos que podrían afectar su función.

Las manifestaciones a las cuales deben hacer frente requieren propiciar una adecuada gestión de riesgos orientada a las actividades operativas y la dirección estratégica, integrada y coordinada en toda su estructura organizacional. Por tanto, cuando se diseña la estrategia para la evaluación, se debe tomar en cuenta factores que pueden repercutir, tanto externos como internos, pero con especial interés estos últimos que tienden a omitirse o minimizarse. Esta labor debe ser elaborada con la seriedad que merece, considerando las vulnerabilidades ante posibles riesgos; de lo contrario podrían afectar el rumbo institucional de forma fortuita e imprevisible.

Décadas atrás, el panorama de instituciones públicas, en cuenta las universidades estatales eran más estable y menos expuesto a la presencia de un conjunto de fenómenos sociales, políticos, ambientales, culturales, científico-tecnológicos y, sobre todo, fenómenos económicos que les plantean un escenario complejo, dependiente y turbulento. Nadie pone en duda la relevancia de su aporte a la sociedad en el desarrollo y la solución de los problemas existentes; no obstante, esto se deja de lado cuando existen otros intereses económicos y políticos.

El control interno y la evaluación de riesgos en las entidades

Generalmente la administración del sector privado y público entra en etapas de pasividad hasta que se generan eventos disruptivos que motivan a repensar cómo se viene actuando, y en múltiples casos, cuando ya los riesgos se han materializado.

Nuestro país, motivado también por eventos de corrupción, acoge los principios del marco de control interno COSO, y promulga en el año 2002 la Ley General de Control Interno, que viene a establecer la obligatoriedad de que las instituciones públicas dispongan de un sistema de control interno, siguiendo los elementos o componentes funcionales y orgánicos que establece la normativa.

Tanto el marco COSO como la Ley de Control Interno, establecen entre sus componentes la evaluación del riesgo, que se puede definir como un proceso dinámico e iterativo para identificar y evaluar los riesgos de cara a la consecución de los objetivos, en todos los niveles de la organización.

Si bien todos los principios del COSO que rigen el componente de Evaluación del Riesgo son importantes, destaco tres a los que debe prestar especial atención las instituciones públicas:

Principio 6. La organización define los objetivos con la suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados.

Como parte de este principio es trascendental la definición de los objetivos asociados a los diferentes niveles de la organización que, aunque no forman parte del proceso de control interno, son la base sobre la que se implementan y llevan a cabo los enfoques de evaluación de riesgo y establecen las actividades de control interno. Cuando los objetivos no son articulados, medibles, alcanzables, pertinentes y, sobre todo, bien claros para quien elabore la evaluación de los riesgos, se pueden tomar decisiones poco acertadas o equivocadas en su definición, omitiendo los verdaderos riesgos y consecuentemente la probabilidad de su materialización.

Principio 7. La organización identifica los riesgos para la consecución de sus objetivos en todos los niveles de la organización y los analiza como base sobre la cual determinar cómo se deben gestionar.

En este proceso, hay que tomar la organización de la institución pública en todo su contexto, especialmente una universidad, que por su naturaleza está conformada por un espectro amplio de actividades, por tanto, no necesariamente la definición de los riesgos y el diseño del proceso para su evaluación deben seguir la misma estructura. La docencia, la investigación, la acción social y la administración tienen riesgos particulares, que deben ser evaluados de acuerdo con su dinámica, actividad y objetivos, por lo que es importante revisar que sean apropiados al giro de su actividad .

Principio 9. La organización identifica y evalúa los cambios que podrían afectar significativamente al sistema de control interno.

Las instituciones públicas están, al igual que las empresas privadas, sujetas a los vaivenes económicos, políticos, regulatorios y sectoriales, por lo que las necesidades y modelo de negocio se deben revisar, adaptar y evolucionar. Como parte de la evaluación del riesgo, la dirección debe identificar los cambios que podrían impactar significativamente el sistema de control interno de la organización y adoptar medidas necesarias con la oportunidad que se requiere.

Debe prestar atención a los cambios externos, sobre todo cuando existan presiones económicas y regulatorias que puedan repercutir en su normal desarrollo. El principio menciona una evaluación rigurosa del modelo de negocio que, para una institución de educación superior, podría interpretarse como la oferta académica, de investigación y acción social, acorde con las necesidades de la sociedad. El gran reto es saber cómo interpretar y satisfacer las necesidades de la sociedad. Pero, ante todo, es de suma relevancia que la definición de los riesgos lo haga un equipo de trabajo que esté involucrado en la toma de decisiones y que conoce perfectamente las actividades que se desarrollan y hacia dónde se dirigen.

Impacto de una adecuada y oportuna gestión de riesgos en una entidad

De la misma forma como hay casos de fracaso, se presentan casos que se pueden catalogar de éxito, y no necesariamente solo en las entidades privadas. Desde una visión muy personal, Correos de Costa Rica puede ser ese caso de éxito. Una entidad que tomó las decisiones apropiadas sobre los riesgos que se le venían presentando a su giro de negocio.

Su modelo de negocio tradicional e, imprescindible para la sociedad costarricense, desde inicios de nuestra independencia, sufre el impacto de la digitalización en las comunicaciones, el internet y las redes sociales.

El volumen de cartas que viajaban por el servicio postal comenzó a decaer año tras año, al punto que la empresa enfrentó su peor crisis financiera en el 2008. Es ahí donde los posibles riesgos se fueron materializando, y no quedaba otra vía que revisar y tomar acciones sobre el giro estratégico de negocio. Apuesta por la diversificación de servicios, enfocada en atender las necesidades que la población venía demandando y busca adaptarse a los hábitos de consumo propios de la época.

A través de los años, la Empresa ha estado identificando las necesidades y realizado un importante esfuerzo para fortalecer sus servicios en procura de satisfacer la demanda de la sociedad. Transformó su negocio hacia el traslado de paquetería e incorporó herramientas tecnológicas que agilizaron los procesos en beneficio de los usuarios.

Fuente: página de Correos de Costa Rica

La empresa ha sabido crear alianzas estratégicas con instituciones públicas y privadas, pilar fundamental en la construcción de un robusto portafolio comercial, que busca contribuir con la descentralización de servicios y adaptar las soluciones a las nuevas tendencias del mercado. Conforme se presentan oportunidades de negocio, ha ido sumando servicios a su cartera de "outsourcing" que impulsan el desarrollo de diferentes áreas.

Podemos decir que su estructura organizacional en sus diferentes niveles, junto con el Comité de Estrategia y Riesgos ha sabido gestionar los riesgos adecuada y oportunamente, pero la tarea no ha terminado, está en constante desarrollo. Desde una visión externa, podría deducirse que Correos de Costa Rica supo conformar un Comité de Estrategia y Riesgos que, en conjunto con los esfuerzos de toda la organización, lograron evadir los embates de lo que pudo haber significado el cierre de una emblemática institución.

Coordinación de los componentes del Control Interno

El control interno no se limita a uno o varios eventos, es un proceso dinámico e iterativo, presente en todas las actividades de una entidad y acorde con las directrices de sus autoridades superiores.

El sistema de control interno debe estar en constante transformación, producto de los cambios de los objetivos, de los controles que se vuelvan obsoletos; o bien, que cambien los riesgos o aparezcan nuevos. Esto implica una permanente supervisión o seguimiento a cada uno de los elementos del control, con el fin de evidenciar que sean vigentes y efectivos.

No sería apropiado para el logro de los objetivos, si se implementa una adecuada evaluación de riesgos, pero no se le da la supervisión a su funcionamiento y efectividad. Es necesario verificar que cada uno de los actores, proceda con en análisis adecuado y no se convierta en una labor más por rutina, que por un trabajo profesional.

La evaluación de riesgos es una herramienta trascendental para el logro de los objetivos institucionales, pero por sí sola no tiene los efectos necesarios, si no se logra el desarrollo de los demás elementos del control interno. Debe existir una coordinación entre la evaluación del control interno, el ambiente de control, las actividades de control, la información y comunicación y el monitoreo o seguimiento. Ninguno de los elementos es más importante que los otros, por lo que es imperativo que sean gestionados apropiadamente, involucrando a todos los integrantes de la entidad.

Para esa adecuada coordinación de los elementos del control interno, es fundamental que desde el puesto más alto se trabaje en desarrollar una cultura de riesgos, que involucre la formulación de las normas, políticas y procedimientos de control, los valores, las actitudes, los conocimientos y los comportamientos de todo el equipo.

Solo de esa forma podría garantizarse que el control interno no se convierta en un sistema inoportuno e ineficaz.

Referencias:

- Committe of Sponsoring Organizations of the Treadway Commision. (2013). Control Interno. Marco Integrado. España
- www.coso.org/aboutus.htm
- Https://correos.go.cr
- La Gran Estafa de Kodak (youtube.com), Jaime García. 2024
- Drew - Business Insights. El Caso Nokia: Caída y ascenso. Vlog wearedrew.co. 2024

Control Interno

BOLETÍN TÉCNICO **2019**

Nota: Los artículos en este Boletín Técnico son aportes de funcionarios de la Oficina de Contraloría Universitaria, sin embargo, no corresponden a pronunciamientos oficiales de ésta.

Lo invitamos a visitar nuestro sitio web **http://www.ocu.ucr.ac.cr** en la que podrá obtener información sobre la función de auditoría, temas de interés para la administración universitaria; incluso puede remitirnos sus observaciones y sugerencias.

Comuníquese con nosotros si desea que se considere un artículo para publicar en este boletín.

Publicación periódica de la Oficina de Contraloría Universitaria

Teléfonos: 2511-1433 **Fax:** 2224-3670
Correo electrónico: **contraloria.universitaria@ucr.ac.cr**
Sitio web: **http://www.ocu.ucr.ac.cr**

Contraloría Universitaria
UCR